

# DPIA op Nextcloud Enterprise

## SURF Vendor Compliance

---

Dit is een vrijblijvende vertaling. Bij tegenstrijdigheden tussen deze vertaling en het originele document is het originele document leidend.

Auteurs: Sjoera Nas (Privacy Company), Julian Rill en Shiyona Keenakkottil (SURF)  
Versie: 1.0  
Datum: 16 juli 2026

Deze publicatie valt onder een Creative Commons Naamsvermelding 4.0 Internationaal-licentie.

## Samenvatting

Dit document is een DPIA (Data Protection Impact Assessment) op de Nextcloud Enterprise Office-software. De DPIA is opgesteld in opdracht van SURF, de samenwerkingsorganisatie voor IT in het Nederlandse hoger onderwijs en onderzoek, soms afgekort tot 'de Nederlandse onderwijssector' of 'onderwijsinstellingen'. Het rapport is geschreven door Privacy Company in samenwerking met SURF.

### Nextcloud-software

Nextcloud Enterprise is een open-source softwaresuite. Organisaties die deze software willen gebruiken, moeten de software zelf hosten of een externe hostingprovider zoeken. De software wordt ontwikkeld en onderhouden door het Duitse bedrijf Nextcloud GmbH, met hulp van externe softwareontwikkelaars. Nextcloud biedt Nextcloud Enterprise zelf niet aan als clouddienst, maar verwijst wel naar Nextcloud-partners die de software als volledig beheerde SaaS kunnen aanbieden.

### Reikwijdte van de DPIA

De reikwijdte van deze DPIA is beperkt tot Nextcloud Files (bestanden delen), Groupware (e-mail, agenda, contacten en dia's), Talk (videoconferenties en chat) en Nextcloud Office (getest met Collabora Online). Daarnaast heeft SURF de generatieve AI-transcriptiefunctie voor videogesprekken in Talk getest. Eindgebruikers hebben via een webinterface toegang tot de verschillende Nextcloud-softwarepakketten. SURF heeft ook getest met Files en Talk geïnstalleerd op Windows en op macOS. Deze DPIA omvat een beveiligingsbeoordeling (hoofdstuk 6).

### Resultaat: 15 lage risico's op het gebied van gegevensbescherming

De uitkomst van deze DPIA is dat er 15 lage gegevensbeschermingsrisico's zijn. De risico's en risicobeperkende maatregelen worden nader toegelicht in de tabel aan het einde van deze samenvatting. Daarnaast bevat deze DPIA een voorlopige lijst met essentiële beveiligingsmaatregelen die organisaties moeten nemen om gegevensbeschermingsrisico's te voorkomen wanneer zij besluiten de software zelf te hosten ([paragraaf C.1.1.1](#)).

### Persoonsgegevens

Deze DPIA is gebaseerd op een juridische analyse van de beschikbare openbare documentatie over de geteste Nextcloud-software, de antwoorden van Nextcloud op vragen van SURF, de inhoud van de onderhandelde gewijzigde verwerkersovereenkomst (Data Processing Agreement, DPA), de bevindingen in de technische bijlage en deel A van de DPIA, evenals een technisch onderzoek van de uitgaande netwerkgegevens.

Om meer inzicht te krijgen in de gegevensverwerking, zowel binnen de software als in de gegevens die met Nextcloud worden gedeeld, heeft SURF de software zelf gehost, twee eindgebruikers en één beheerder (hierna: admin) aangemaakt en een aantal vooraf gedefinieerde scenario's met de drie gebruikers uitgevoerd. SURF heeft ook de beschikbare logbestanden in de software geraadpleegd en een verzoek om inzage ingediend bij Nextcloud.

In dit rapport wordt onderscheid gemaakt tussen vijf categorieën persoonsgegevens die binnen de software worden verwerkt of door Nextcloud GmbH worden verwerkt:

1. Inhoudelijke gegevens (alleen beschikbaar voor klanten, binnen de zelfgehoste Nextcloud-software)
2. Accountgegevens, in twee soorten:
  - a. Beheerdersaccountgegevens
  - b. Contactgegevens van inkoopmedewerkers
3. Diagnostische gegevens, in drie soorten:
  - a. Logs die alleen beschikbaar zijn voor klanten
  - b. Logs die klanten optioneel met Nextcloud delen
  - c. Logs aangemaakt door Nextcloud GmbH
4. Ondersteuningsgegevens (zowel de inhoud van tickets als metagegevens)
5. Websitegegevens, in twee soorten:
  - a. de websites met beperkte toegang, d.w.z. het beheer- en ondersteuningsportaal, en
  - b. de openbaar toegankelijke pagina's op nextcloud.com met relevante technische documentatie, het formulier om inzage te vragen en juridische informatie.

Een belangrijk verschil met cloudproviders van productiviteitssoftware is dat het bedrijf Nextcloud zeer weinig persoonsgegevens verzamelt. Nextcloud heeft de softwareapplicaties bijvoorbeeld niet zo geprogrammeerd dat ze automatisch telemetriegegevens naar het bedrijf verzenden en heeft geen toegang tot gegevens die in de klantomgeving worden verwerkt, zelfs niet voor ondersteuningsdoeleinden.

### **Doeleinden, rollen en rechtsgrondslagen**

Aanvankelijk stelde Nextcloud zich op het standpunt dat het uitsluitend als verwerker optrad voor de inhoud van supporttickets. Uit de technische analyse bleek echter dat Nextcloud meer categorieën persoonsgegevens verwerkte. Naar aanleiding van de onderhandelingen met SURF heeft Nextcloud ermee ingestemd om ook als verwerker op te treden voor de beperkte hoeveelheid persoonsgegevens die het verzamelt: beheerdersaccountgegevens, diagnostische gegevens en websitegegevens met beperkte toegang. Nextcloud mag deze persoonsgegevens verwerken voor vier specifieke doeleinden, namelijk:

1. Het technisch beschikbaar stellen van de software en applicaties via portal.nextcloud.com (verwerken van bezoekers- en downloadgegevens);
2. Het bieden van derdelijsondersteuning/technische assistentie op basis van verzoeken van klanten;
3. Het helpen beveiligen van de door de klant in de software verwerkte persoonsgegevens door het verzenden van updatemeldingen en nieuwsbrieven over technische updates en beveiligingsontwikkelingen aan beheerders;
4. Technische verbetering van de software en diensten voor alle klanten, inclusief het verhelpen van bugs, het oplossen van problemen, het aanbrengen van patches en algemeen onderhoud, door gebruik te maken van de geaggregeerde ondersteuningsgegevens en vrijwillig verstrekte diagnostische gegevens.

Aangezien elke leverancier bepaalde persoonsgegevens van zijn klanten moet gebruiken voor zijn eigen legitieme zakelijke doeleinden, bijvoorbeeld om facturen te versturen, zijn SURF en Nextcloud ook een beperkte lijst van zeven specifieke toegestane doeleinden voor

*verdere verwerking* overeengekomen. Dit betekent dat Nextcloud deze gegevens als verwerkingsverantwoordelijke mag verwerken, wanneer dit strikt noodzakelijk en evenredig is voor deze doeleinden, en binnen de voorwaarden die zijn overeengekomen in de gewijzigde verwerkersovereenkomst. In verkorte vorm zijn deze zeven doeleinden:

1. Naleving van wettelijke verplichtingen
2. Facturering, uitvoering van bestellingen en ontvangst van betalingen
3. Klantrelatiebeheer
4. Naleving van licentievoorwaarden/fraudedetectie
5. Gebruik statistische gegevens voor interne rapportage, financiële rapportage, het prioriteren van beveiligingspatches en productstrategie
6. Het maken van statistische websiteanalyses op basis van de websites met beperkte toegang.
7. Gebruik statistische gegevens om de prestaties en efficiëntie van de software technisch te verbeteren en te optimaliseren

Deze DPIA concludeert dat verdere verwerking voor deze doeleinden *verenigbaar* is met de doeleinden waarvoor Nederlandse onderwijsinstellingen Nextcloud als verwerker toestaan om persoonsgegevens te verzamelen, in overeenstemming met de vereisten van artikel 6, lid 4, van de AVG.

#### **Internationale gegevensoverdrachten**

Nextcloud streeft ernaar het enige serieuze Europese alternatief voor Microsoft en Google te zijn en benadrukt gegevenssovereiniteit als een belangrijke reden om voor zijn producten te kiezen. Nextcloud garandeert contractueel dat het verzoeken om openbaarmaking van overheidsinstanties buiten de EU zal afwijzen en de overeengekomen maatregelen zal nemen om openbaarmaking aan EU-autoriteiten te voorkomen of op zijn minst tot een minimum te beperken. Nextcloud heeft tevens uitgebreide garanties gegeven dat het geen achterdeurtjes in de software heeft ingebouwd – en dat ook niet zal doen – die tot toegang voor overheidsinstanties zouden kunnen leiden. De beveiliging van de software is onlangs gecontroleerd door de Duitse cyberbeveiligingsautoriteit BSI, en Nextcloud heeft een CSPN-certificaat ontvangen.

Nextcloud maakt echter gebruik van een leverancier uit de VS voor de verzending van uitgaande e-mail. Tijdens het testen werd de beheerder automatisch geabonneerd op zowel een beveiligingsnieuwsbrief als een commerciële nieuwsbrief van Nextcloud, en de beheerder en Nextcloud hebben hierover gecommuniceerd in het kader van deze DPIA. Deze Amerikaanse leverancier houdt logboeken bij met de inhoud van de e-mails plus gedetailleerde technische informatie over de ontvanger. Nextcloud zal in het derde kwartaal van 2026 overstappen op een leverancier uit de EU.

SURF maakte gebruik van de Office-software van Nextcloud, die is gebaseerd op Collabora Online van het Britse bedrijf Collabora. Dit betekent dat medewerkers van Collabora in het Verenigd Koninkrijk toegang hebben tot de relevante ondersteuningstickets in het centrale ticketsysteem van Nextcloud. Nextcloud heeft toegezegd om alleen toegang te verlenen aan medewerkers die in de EU gevestigd zijn, mocht het adequaatheidsbesluit voor het Verenigd Koninkrijk ongeldig worden.

Daarnaast maakt Nextcloud gebruik van twee Amerikaanse softwarebibliotheken voor essentiële beveiligingsupdates en informatie: GitHub en Hugging Face (om een LLM voor Nextcloud Assistant te downloaden). Deze DPIA beveelt maatregelen aan voor beheerders om tracking door deze platforms te voorkomen.

### Bewaring van gegevens en uitoefening van rechten van betrokkenen

Nextcloud heeft snel en gedetailleerd gereageerd op de verzoeken om inzage van betrokkenen (DSAR's) van SURF. Er ontbraken echter vier categorieën persoonsgegevens. Nextcloud heeft de ontbrekende persoonsgegevens tijdens het DPIA-proces verstrekt en toegezegd om in de toekomst volledig te reageren op DSAR's.

Nextcloud en SURF zijn een bewaartermijn van 15 maanden overeengekomen voor ondersteuningstickets na afsluiting van de zaak. Beheerders kunnen Nextcloud vragen om tickets en bijlagen eerder te verwijderen.

Uit de technische analyse blijkt dat Nextcloud GmbH en zijn subverwerkers zeven soorten logbestanden kunnen verwerken. Nextcloud heeft de bewaartermijnen aan SURF toegelicht en heeft toegezegd de details in juli 2026 te publiceren, na goedkeuring door SURF. Ook heeft Nextcloud toegezegd de centrale documentatie te verbeteren over de vele logbestanden die binnen de software kunnen worden gegenereerd, en de standaard bewaartermijnen (of standaard maximale opslaggroottes) daarvan.

### Conclusies

Op basis van de gewijzigde verwerkersovereenkomst voor de Nederlandse onderwijssector fungeert Nextcloud als verwerker voor de vier relevante categorieën persoonsgegevens voor de vier overeengekomen doeleinden, en als geautoriseerde verwerkingsverantwoordelijke voor een deel van deze persoonsgegevens voor de overeengekomen en daarmee verenigbare zeven *aanvullende* verwerkingsdoeleinden. De gewijzigde DPA waarborgt dat de onderwijsinstellingen de controle behouden over de verwerking via subverwerkers, kunnen vertrouwen op gegevensverwerking die uitsluitend binnen de EU plaatsvindt (plus de verwerking van ondersteuningstickets in het Verenigd Koninkrijk indien zij kiezen voor Collabora Online), zelf de noodzakelijke bewaartermijnen kunnen vaststellen, alleen strikt noodzakelijke cookies accepteren, en erop kunnen vertrouwen dat SURF het recht uitoefent om de naleving van de overeengekomen gegevensbeschermingsclausules en -maatregelen te controleren.

Zoals blijkt uit de onderstaande tabel zijn er, op basis van de reeds door Nextcloud genomen maatregelen en op voorwaarde dat de onderwijsinstellingen de aanbevolen maatregelen toepassen en Nextcloud de overeengekomen maatregelen neemt, geen hoge gegevensbeschermingsrisico's meer bekend, en slechts 15 lage of opgeloste risico's.

| Aantal | Risico's                     | Aanbevolen maatregelen voor onderwijsinstellingen                                 | Maatregelen die door NEXTCLOUD zijn genomen of toegezegd                                           | Resterende risico's |
|--------|------------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|---------------------|
| 1.     | Verlies van controle over de | Meld je aan voor Nextcloud Enterprise via SURF, en zorg er bij aanmelding via een | Overeenstemming bereikt over beperkende lijst van vier verwerkingsdoeleinden in de gewijzigde DPA. | opgelost            |

|    |                                                                                                                                      |                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                     |      |
|----|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
|    | verwerking van beheerdersaccountgegevens in Accountgegevens, Diagnostische gegevens, Meta-Ordersteuningsgegevens, en Websitegegevens | reseller of aanbieder van een volledig beheerde oplossing voor dat de SURF-DPA van toepassing is.                                                      | Overeenstemming bereikt over een limitatieve lijst van zeven toegestane doeleinden voor verdere verwerking (legitieme bedrijfsactiviteiten) in de gewijzigde DPA.                                                                                                                                                                                   |      |
|    |                                                                                                                                      |                                                                                                                                                        | Overeenstemming bereikt over drie expliciete verwerkingsverboden: geen verdere verwerking voor andere doeleinden, geen verwerking voor reclamedoel-einden of het aanbieden van advertenties, niet voor direct marketing, profilering, onderzoek of analytische doeleinden, tenzij de klant Nextcloud hiertoe opdracht geeft, en geen CSAM-scanning. |      |
|    |                                                                                                                                      | (SURF): gebruik van het auditrecht om de naleving van de doelbinding, gegevensminimalisatie en bewaartermijnen te controleren.                         | Er is overeenstemming bereikt over een uitgebreid auditrecht voor SURF namens de onderwijsinstellingen in de gewijzigde DPA.                                                                                                                                                                                                                        |      |
|    |                                                                                                                                      |                                                                                                                                                        | Toezegging gedaan om de beveiligingsaudit voor CSPN om de drie jaar te herhalen en de volledige bevindingen met SURF te delen.                                                                                                                                                                                                                      |      |
| 2. | Verlies van controle bij de doorgifte van e-mailadressen naar de VS                                                                  | -                                                                                                                                                      | Toezegging gedaan om in het derde kwartaal van 2026 over te stappen op een in de EU gevestigde e-mailprovider.                                                                                                                                                                                                                                      | laag |
|    |                                                                                                                                      | Beheerders instrueren om te voorkomen dat zij hun privé-IP-adressen en persoonlijke apparaatgegevens delen bij het gebruik van GitHub en Hugging Face. | Nextcloud verwerkt als verwerker gegevens uitsluitend binnen de EU, zoals overeengekomen in de gewijzigde DPA, met uitzondering van door klanten gekozen subverwerkers buiten de EU, zoals Collabora.                                                                                                                                               |      |
|    |                                                                                                                                      | Geef beheerders de instructie om niet permanent ingelogd te blijven op GitHub en Hugging Face.                                                         | Nextcloud zal in het derde kwartaal van 2026 twee soorten abonnementen aanbieden aan Enterprise-klienten: als commercieel contactpersoon voor een klant of als beheerder.                                                                                                                                                                           |      |

|    |                                                                                                                     |                                                                                                                                                                                   |                                                                                                                                                                           |          |
|----|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 3. | Verlies van controle bij doorgifte van Ondersteuningsgegevens naar Collabora buiten de EU                           | -                                                                                                                                                                                 | De toegang tot de relevante Collabora-tickets in Zammad is beperkt tot medewerkers die zich fysiek in het Verenigd Koninkrijk en in de EU bevinden.                       | opgelost |
|    |                                                                                                                     |                                                                                                                                                                                   | Toezegging gedaan om toegang door medewerkers in het Verenigd Koninkrijk te blokkeren als de adequaatheidsstatus ongeldig wordt.                                          |          |
| 4. | Verlies van vertrouwelijkheid door een beveiligingsinbreuk                                                          | -                                                                                                                                                                                 | Nextcloud zal 2FA afdwingen op het beheer- en ondersteuningsportaal in de nieuwe versie v7.1 van het ondersteuningsportaal van Zammad, die op 1 juli 2026 is uitgebracht. | opgelost |
| 5. | Verlies van controle door gebrek aan transparantie: Diagnostische gegevens worden optioneel gedeeld door beheerders | Optioneel: overweeg het gebruik van gepseudonimiseerde beheerdersaccounts, bijvoorbeeld door middel van identiteitsfederatie om gebruiksonderzoeksgegevens te delen met Nextcloud | Er is overeengekomen om Diagnostische gegevens op te nemen in de uitgebreide reikwijdte van de gewijzigde DPA.                                                            | laag     |
|    |                                                                                                                     |                                                                                                                                                                                   | Bewaartermijnen voor 3 soorten logbestanden die optioneel door beheerders worden gedeeld, zijn overeengekomen in de gewijzigde DPA.                                       |          |
|    |                                                                                                                     |                                                                                                                                                                                   | Deze bewaartermijnen zullen in juli 2026 openbaar worden vastgelegd.                                                                                                      |          |
| 6. | Verlies van controle door gebrek aan transparantie en risico                                                        | (SURF): audits uitvoeren op de naleving van doelbinding, gegevensminimalisatie en bewaartermijnen, zowel als verwerker als geautoriseerde verwerkingsverantwoordelijke.           | Er is overeengekomen dat SURF uitgebreide auditmogelijkheden krijgt in de gewijzigde DPA.                                                                                 | laag     |
|    |                                                                                                                     | Beheerders informeren over de functionele cookies via deze overkoepelende DPIA en hen instrueren de standaardinstellingen op de openbare                                          | De informatie over functionele cookies op het beheerders- en ondersteuningsportaal wordt in juli 2026 bijgewerkt                                                          |          |

|    |                                                                                                                               |                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |          |
|----|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|    | op heridentificatie van andere Diagnostische gegevens, activiteitenlogboeken van het ondersteuningssysteem en Websitegegevens | website nextcloud.com niet te wijzigen.                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |          |
|    |                                                                                                                               | Breng beheerders op de hoogte van het bestaan van de zeven geïdentificeerde relevante logbestanden die door Nextcloud GmbH en haar subverwerkers worden genereerd, en van de bewaartermijnen. | Nextcloud heeft SURF aanvullende informatie verstrekt over de zeven logbestanden. Nextcloud zal deze informatie in juli 2026 op zijn openbare website publiceren (zoals goedgekeurd door SURF).                                                                                                                                                                                                                                                               |          |
|    |                                                                                                                               | Informeer beheerders over de inhoud van het activiteitenlogboek van het Zammad-supportticketsysteem en de bewaartermijn van 42 dagen.                                                         | Nextcloud zal deze informatie in juli 2026 op zijn openbare website publiceren (zoals beoordeeld door SURF).                                                                                                                                                                                                                                                                                                                                                  |          |
| 7. | Verlies van controle en gebrek aan transparantie bij subverwerkers                                                            | -                                                                                                                                                                                             | Er is overeenstemming bereikt over de procedure voor het omgaan met wijzigingen in de gewijzigde DPA, zowel met betrekking tot nieuwe subverwerkers als tot andere wijzigingen.                                                                                                                                                                                                                                                                               | opgelost |
| 8. | Onvermogen om betrokkenerechten uit te voeren                                                                                 | -                                                                                                                                                                                             | Toezegging gedaan om volledige toegang te verlenen bij een inzageverzoek. Dit omvat toegang tot alle verzamelde gebruiksonderzoeksgegevens, activiteitenlogboeken van het ondersteuningsticketsysteem, bevroren webservertoegangslogboeken (op voorwaarde dat Nextcloud de identiteit van de betrokkene op betrouwbare wijze kan verifiëren) en logboeken die worden bijgehouden door Postmark (of een toekomstige in de EU gevestigde e-maildienstverlener). | laag     |

|     |                                                                                                     |                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |      |
|-----|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
|     |                                                                                                     |                                                                                                                                                                                             | <i>OPMERKING: SURF heeft dit niet opnieuw getest met een nieuw DSAR.</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |      |
| 9.  | Onvermogen om het recht van de betrokkene op verwijdering van Ondersteuningsgegevens uit te oefenen | Geef beheerders de instructie om in ondersteuningstickets alleen strikt noodzakelijke persoonsgegevens te delen. Gebruik tickets niet om juridische of financiële vorderingen in te dienen. | <p>Nextcloud zal over het algemeen voldoen aan verzoeken tot verwijdering van een of meer ondersteuningstickets en/of bijlagen, tenzij er een wettelijke reden is om een specifiek ticket te bewaren.</p> <p>Nextcloud heeft voor SURF-leden een maximale bewaartermijn van 15 maanden overeengekomen voor afgesloten supporttickets.</p> <p>In de overeengekomen nieuwe openbare documentatie over de logbestanden die Nextcloud GmbH verzamelt en de bewaartermijnen staat vermeld dat Nextcloud de supporttickets over een specifiek onderwerp bij wijze van uitzondering langer mag bewaren, om een specifieke juridische reden.</p> <p>Nextcloud heeft al een waarschuwing tegen het delen van persoonsgegevens in bijlagen op het beheerdersportaal geïmplementeerd en zal de waarschuwing uiterlijk in het derde kwartaal van 2026 ook op het supportportaal weergeven.</p> | laag |
|     |                                                                                                     | Geef beheerders de instructie om Nextcloud jaarlijks te verzoeken alle supporttickets te verwijderen na de zelf vastgestelde bewaartermijn van bijvoorbeeld 13 of 15 maanden.               | Overeengekomen in de gewijzigde DPA om als geautoriseerde verwerkingsverantwoordelijke uitsluitend geaggregeerde en gepseudonimiseerde gegevens uit supporttickets te verwerken die boven het tenant-niveau liggen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |      |
| 10. | Bekendmaking van verlies van controle over                                                          |                                                                                                                                                                                             | In de gewijzigde DPA is overeengekomen om de voorgestelde maatregelen ter risicobeperking te nemen. Nextcloud zal verzoeken van autoriteiten buiten                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | laag |

|     |                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                        |          |
|-----|------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|     | (beperkte) persoonsgegevens aan overheidsinstanties binnen en buiten de EU                           |                                                                                                                                                                                                                                                                                                                                                                                                                             | <p>de EU afwijzen. Nextcloud zal trachten verzoeken van EU-autoriteiten door te sturen naar zijn klant, deze waar mogelijk en haalbaar juridisch aanvechten, maar indien nodig slechts de minimaal noodzakelijke gegevens verstrekken.</p> <p>In de gewijzigde DPA is toegezegd om ten minste eenmaal per jaar transparantiestatistieken te publiceren, inclusief cijfers over ontvangen en beantwoorde verzoeken.</p> |          |
| 11. | Verlies van controle over verwerkingen van Nextcloud als onafhankelijke verwerkingsverantwoordelijke | <p>Waarschuw beheerders om hun beheerdersaccountgegevens niet te gebruiken om verwerking door Nextcloud of derden als onafhankelijke verwerkingsverantwoordelijke mogelijk te maken, bijvoorbeeld door toestemming te geven voor analytische en trackingcookies. Raad beheerders aan een pseudoniem account te gebruiken bij het registreren voor een evenement of bij het registreren om een whitepaper te downloaden.</p> | <p>Er is overeenstemming bereikt over twee lijsten met doeleinden in de gewijzigde DPA.</p> <p>In de gewijzigde DPA is overeengekomen om de huidige standaardinstellingen voor privacy te handhaven. Analyse- en marketingcookies worden alleen op de openbare website geplaatst na vrijwillige toestemming van de gebruiker.</p>                                                                                      | opgelost |
| 12. | Verlies van controle: gebruik van trackingpixels in uitgaande e-mail van Nextcloud                   | .                                                                                                                                                                                                                                                                                                                                                                                                                           | Nextcloud heeft de trackingpixel in zijn emails uitgeschakeld.                                                                                                                                                                                                                                                                                                                                                         | opgelost |

|     |                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                             |      |
|-----|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| 13. | Verlies van controle over gegevens van beheerdersaccounts in nieuwsbrieven                                   | Geef beheerders de instructie om zich af te melden voor commerciële nieuwsbrieven.                                                                                                                                                                                                                                                                                                            | In het Nextcloud-zelfbedieningsportaal (portal.nextcloud.com) kunnen klanten zich in het derde kwartaal van 2026 registreren als beheerder of commercieel contactpersoon en zelf beslissen of ze zich willen aan- of afmelden voor commerciële en technische nieuwsbrieven. | laag |
| 14. | Verlies van controle door gebrek aan transparantie over het bestaan van meerdere logbestanden in de software | Gebruik de lijst in deze overkoepelende DPIA om beheerders bewust te maken van alle beschikbare logbestanden.                                                                                                                                                                                                                                                                                 | Nextcloud zal in het derde kwartaal van 2026 in de <a href="#">bestaande logboekdocumentatie</a> een beter overzicht van de beschikbare logboeken voor beheerders bieden.                                                                                                   | laag |
| 15. | Chilling effect: monitoringsysteem voor medewerkers en studenten                                             | Maak beheerders bewust van de potentieel gevoelige inhoud van de (oorspronkelijke) audit- en Talk-interactielogboeken.                                                                                                                                                                                                                                                                        | Nextcloud heeft toegezegd om tegen eind 2026 een tweede exportversie van de audit- en interactielogboeken te ontwikkelen. Persoonsgegevens zoals vergader- en bestandsnamen worden gemaskeerd met ***VERWIJDERDE GEVOELIGE WAARDE***.                                       | laag |
|     |                                                                                                              | Pas het interne IT-beleid aan om vast te leggen wanneer en voor welke doeleinden deze logbestanden legitiem mogen worden gebruikt.<br><br>Om te voorkomen dat de audit- en interactielogboeken worden gebruikt als monitoring-systeem voor medewerkers, moet de gemaskeerde versie van de audit- en Talk-interactielogboeken in de SIEM- en logboekbeheertools worden geïmporteerd zodra deze | Nextcloud zal de beschikbare informatie over de gevoelige inhoud in het derde kwartaal van 2026 bijwerken.                                                                                                                                                                  |      |

|  |  |                                                                                              |  |  |
|--|--|----------------------------------------------------------------------------------------------|--|--|
|  |  | beschikbaar is, en moet een passende bewaartermijn voor de ruwe gegevens worden vastgesteld. |  |  |
|--|--|----------------------------------------------------------------------------------------------|--|--|

## Part C Beschrijving en beoordeling van risico's voor betrokkenen

### C.1 Risico's voor betrokkenen

Dit deel betreft de beschrijving en beoordeling van de risico's voor betrokkenen. Dit deel begint met een algemene inventarisatie van de risico's voor de rechten en vrijheden van betrokkenen als gevolg van de verwerking van de beperkte persoonsgegevens door Nextcloud als verwerker en als geautoriseerde verwerkingsverantwoordelijke. De risico's worden vervolgens ingedeeld op basis van de waarschijnlijkheid dat ze zich voordoen en de gevolgen voor de rechten en vrijheden van de betrokkenen wanneer ze zich voordoen.

Dit deel bevat twee verschillende lijsten met risico's en risicobeperkende maatregelen. De eerste lijst bevat een voorlopige opsomming van risico's op het gebied van gegevensbescherming en informatiebeveiliging die kunnen voortvloeien uit implementatie- en configuratiekeuzes die de onderwijsinstelling maakt bij de implementatie van de Nextcloud Enterprise-software.

De hoofdanalyse in paragraaf C.2 analyseert de waarschijnlijkheid en impact van de risico's die voortvloeien uit de gegevensverwerking door Nextcloud, met inbegrip van de standaardinstellingen voor het aanmaken van logbestanden met diagnostische gegevens in de zelfgehoste omgeving en de bewaartermijnen daarvan, en houdt rekening met alle juridische, technische en organisatorische maatregelen die door Nextcloud zijn of zullen worden toegepast om de geïdentificeerde risico's te beperken.

#### C.1.1 Identificatie van risico's

Deze DPIA identificeert 15 specifieke gegevensbeschermingsrisico's die voortvloeien uit de verwerking door Nextcloud, met inbegrip van de softwaremogelijkheden en configuratieopties voor de onderwijsinstellingen.

De gegevensbeschermingsrisico's kunnen in de volgende categorieën worden ingedeeld:

- het onvermogen om rechten uit te oefenen (met inbegrip van, maar niet beperkt tot, privacyrechten)
- het onvermogen om toegang te krijgen tot diensten of mogelijkheden
- verlies van controle over het gebruik van persoonsgegevens
- discriminatie
- identiteitsdiefstal of -fraude
- financieel verlies
- reputatieschade
- fysiek letsel
- verlies van vertrouwelijkheid
- heridentificatie van gepseudonimiseerde gegevens of
- enige andere aanzienlijke economische of sociale nadelen<sup>1</sup>

<sup>1</sup> Lijst verstrekt door de ICO, stap 5, URL: <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/>

Deze risico's moeten worden beoordeeld in het licht van de waarschijnlijkheid dat ze zich voordoen en de ernst van de gevolgen.

De Britse gegevensbeschermingscommissie ICO geeft de volgende richtlijnen: *Schade hoeft niet onvermijdelijk te zijn om als risico of als hoog risico te worden aangemerkt. De kans moet groter zijn dan verwaarloosbaar klein, maar elke significante mogelijkheid van zeer ernstige schade kan al voldoende zijn om als hoog risico te worden aangemerkt. Evenzo kan een hoge waarschijnlijkheid van wijdverspreide maar minder ernstige schade nog steeds als hoog risico worden beschouwd.*<sup>2</sup>

Om de ernst van de gevolgen en de waarschijnlijkheid van de schade voor deze algemene risico's af te wegen, combineert dit rapport een lijst van specifieke risico's met de specifieke omstandigheden van de onderzochte gegevensverwerking.

Tabel1 : Risicoscorematrix<sup>3</sup>

|                                                  |                 |             |                  |                           |
|--------------------------------------------------|-----------------|-------------|------------------|---------------------------|
| <b>Ernst van de impact</b>                       | Ernstige impact | Laag risico | Hoog risico      | Hoog risico               |
|                                                  | Enige impact    | Laag risico | Gemiddeld risico | Hoog risico               |
|                                                  | Minimale impact | Laag risico | Laag risico      | Laag risico               |
|                                                  |                 | Heel klein  | Redelijke kans   | Waarschijnlijker dan niet |
| <b>Waarschijnlijkheid van schade (voorkomen)</b> |                 |             |                  |                           |

#### C.1.1.1 Verwerking van persoonsgegevens in de Nextcloud Enterprise-software

Zoals vermeld in de inleiding van dit hoofdstuk C, bevat dit hoofdstuk een voorlopige lijst van risico's op het gebied van gegevensbescherming en informatiebeveiliging die door de onderwijsinstelling zelf kunnen worden beperkt, indien zij besluit de Nextcloud Enterprise-software zelf te hosten.

Deze overkoepelende DPIA kan geen adequaat overzicht bieden van alle mogelijke interne risico's op het gebied van gegevensbescherming, die verband houden met de beveiligingsconfiguratie en de specifieke doeleinden waarvoor faculteiten/afdelingen de software mogelijk willen gebruiken voor verschillende categorieën persoonsgegevens, aangezien deze risico's in hoge mate afhankelijk zijn van de persoonsgegevens en vertrouwelijke gegevens die onderwijsinstellingen in de Nextcloud-software zullen verwerken.

<sup>2</sup> Idem, stap 5.

<sup>3</sup> Zoals vóór de Brexit door de ICO geïntroduceerd en overgenomen door de Nederlandse overheid in haar nationale DPIA-sjabloon.

Deze overkoepelende DPIA kan daarom alleen een overzicht bieden van de algemene risico's die voortvloeien uit het gebruik van Nextcloud. Het is aan de privacyfunctionarissen en functionarissen gegevensbescherming om deze overkoepelende DPIA aan te vullen met specifieke risico's en binnen elke organisatie passende risicobeperkende maatregelen te treffen. Daarom bevat dit hoofdstuk geen beoordeling van de waarschijnlijkheid en de impact van de risico's.

Tabel 2 : potentiële risico's voor zelf gehoste software die door de organisaties zelf kunnen worden beperkt

| Potentiële interne risico's op het gebied van gegevensbescherming                                                                                       | Aanbevolen risicobeperkende maatregelen                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verlies van controle / verlies van vertrouwelijkheid / verlies van beschikbaarheid als gevolg van externe datalekken (waaronder phishing en ransomware) | Vraag de CISO om een risicobeoordeling op te stellen voor de verschillende categorieën gegevens op basis van de risicobereidheid van de organisatie en alle noodzakelijke maatregelen te implementeren (meer dan deze voorlopige lijst)                                |
|                                                                                                                                                         | Zorg voor bekwame systeembeheerders en 24/7 beschikbaarheid van een SOC.                                                                                                                                                                                               |
|                                                                                                                                                         | Bestudeer paragraaf A.6.1 van deze DPIA en implementeer de beschikbare beveiligingsmaatregelen.                                                                                                                                                                        |
|                                                                                                                                                         | Voer regelmatig een penetratietest uit op de zelfgehoste configuratie.                                                                                                                                                                                                 |
|                                                                                                                                                         | Exporteer de Nextcloud-logs naar het eigen SIEM van de organisatie en andere logbeheertools en voer systematische controles uit op de naleving.                                                                                                                        |
|                                                                                                                                                         | Zorg voor een back-up die niet via het live-systeem kan worden gecompromitteerd en zorg ervoor dat er geen persoonsgegevens worden verwerkt in de ontwikkel- en testomgeving van de DTAP.                                                                              |
| Verlies van controle als gevolg van interne datalekken                                                                                                  | Overweeg het gebruik van de 13 privacymaatregelen die worden beschreven in <a href="#">paragraaf A.4.1</a>                                                                                                                                                             |
|                                                                                                                                                         | Implementeer fijnmazige bestandstoegangscontroles. Overweeg beperkingen zoals het verhinderen van toegang tot XLSX-bestanden van de HR-afdeling vanuit IP-bereiken van buiten het bedrijf of het blokkeren van toegang tot specifieke bestanden vanuit niet-EU-landen. |
|                                                                                                                                                         | Houd de gebruikersregistratie in de AD/LDAP up-to-date, aangezien toegang via groepen afhankelijk is van deze registratie.                                                                                                                                             |
|                                                                                                                                                         | Informeer eindgebruikers over de 3 opties die zij hebben om de verwerking van hun persoonsgegevens te beperken ( <a href="#">paragraaf A.4.2</a> ).                                                                                                                    |
| Verlies van controle door een gebrek aan                                                                                                                | Maak onderscheid tussen root- of topbeheerders die toegang hebben tot de ruwe loggegevens, en beheerders die                                                                                                                                                           |

|                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| geautoriseerde beheerders                                                                                                                                                         | toegang hebben tot gemaskeerde logs in het SIEM-systeem van de organisatie en andere logbeheertools.                                                                                                                                                                                                                                                                                                    |
|                                                                                                                                                                                   | Pas het interne IT-beleid aan om vast te leggen welke gegevens beheerders met Nextcloud mogen delen (zoals gebruiksenquête's en rapporten met systeeminformatie).                                                                                                                                                                                                                                       |
| Verlies van controle door gebrek aan transparantie                                                                                                                                | Gebruik deze overkoepelende DPIA en houd de overeengekomen nieuwe openbare documentatie van Nextcloud in de gaten om het interne register van verwerkingsactiviteiten bij te werken, en werk zowel het interne gegevensverwerkingsbeleid/IT-beleid als het externe privacybeleid bij om alle relevante betrokkenen te informeren over de gegevensverwerking door de organisatie zelf en door Nextcloud. |
| Verlies van controle door buitensporige gegevensbewaring                                                                                                                          | Breng orde in de huidige gegevensverwerking door een maximale bewaartermijn vast te stellen voor bestanden die in de Nextcloud-software worden geïmporteerd. Werk de interne registratierichtlijnen en handleidingen voor gegevensverwerking bij met maximale bewaartermijnen, en controleer en handhaaf de naleving hiervan.                                                                           |
| Afschrikkend effect van het systeem voor werknemersmonitoring                                                                                                                     | - Dit wordt besproken in de volgende paragraaf over risico's die door Nextcloud worden veroorzaakt en beperkt.                                                                                                                                                                                                                                                                                          |
| Verlies van controle / verlies van vertrouwelijkheid door ongeoorloofde toegang tot vergaderingen                                                                                 | - Wordt besproken in de volgende paragraaf: dwing het gebruik van de lobbyfunctie centraal af.                                                                                                                                                                                                                                                                                                          |
|                                                                                                                                                                                   | Geef gebruikers de mogelijkheid om E2EE in te schakelen voor vergaderingen in Talk over vertrouwelijke en gevoelige onderwerpen.                                                                                                                                                                                                                                                                        |
| Gebrek aan zekerheid over de integriteit van de software, met als gevolg mogelijke achterdeurtjes in software-updates die leiden tot ongeoorloofde toegang of externe datalekken. | Implementeer DTAP-scheiding (Develop, Test, Acceptance, Production).                                                                                                                                                                                                                                                                                                                                    |
|                                                                                                                                                                                   | Controleer de integriteit van releases met behulp van handtekeningen en cryptografische hashes vóór de implementatie.                                                                                                                                                                                                                                                                                   |
|                                                                                                                                                                                   | Zorg voor gecentraliseerde logboekregistratie en SIEM-monitoring voor het detecteren van afwijkende activiteiten of gegevenslekken.                                                                                                                                                                                                                                                                     |

#### C.1.1.2 Verwerking van persoonsgegevens door Nextcloud (inclusief ontwerpbeslissingen)

Als gevolg van de onderhandelingen met SURF is Nextcloud feitelijk en formeel een verwerker geworden voor de (beperkte) persoonsgegevens in de beheerdersaccountgegevens, Diagnostische gegevens, Ondersteuningsgegevens en Websitegegevens met beperkte toegang. Nextcloud is in de gewijzigde DPA ook gemachtigd om specifieke persoonsgegevens verder te verwerken voor zeven legitieme zakelijke doeleinden, wanneer dit strikt noodzakelijk en evenredig is. Deze contractuele verbeteringen hebben veel hoge gegevensbeschermingsrisico's in verband met een verlies van controle en een gebrek aan doelbinding beperkt.

Nextcloud is trots op zijn open-sourcegegevensverwerking, waardoor EU-klanten volledige controle hebben over de gegevensverwerking binnen de EU. Uit deze DPIA blijkt echter dat Nextcloud in de door SURF geteste opzet momenteel gebruikmaakt van één Amerikaans subverwerker (ActiveCampaign), en dat klanten partners buiten de EU kunnen kiezen, zoals Collabora in het Verenigd Koninkrijk. Nextcloud laat klanten ook de websites van twee Amerikaanse derde partijen (GitHub en Hugging Face) bezoeken om software en noodzakelijke beveiligingsupdates te downloaden. Nextcloud heeft toegezegd in het derde kwartaal van 2026 over te stappen op een in de EU gevestigde e-mailprovider en heeft ingestemd met andere risicobeperkende maatregelen.

Nextcloud heeft ervoor gezorgd dat de software voldoende logbestanden genereert zodat klanten aan hun beveiligingsverplichtingen kunnen voldoen. Deze logbestanden kunnen gevoelige gegevens bevatten, zoals welke student of medewerker wanneer heeft ingelogd en aan welke bestanden zij hebben gewerkt. Om onderwijsinstellingen te helpen onnodige toegang tot deze logbestanden te voorkomen, heeft Nextcloud toegezegd een gemaskeerde versie van de audit- en interactielogbestanden te maken voor export naar de meer algemeen toegankelijke logbeheersystemen binnen een organisatie. Deze maatregel beschermt tegen het afschrikkende effect op gebruikers en beheerders die vrezen dat hun gedragsgegevens worden gemonitord.

Ten slotte heeft Nextcloud toegezegd onderscheid te maken tussen Accountgegevens van beheerders en commerciële contactgegevens, en zal het alleen nieuwsbrieven versturen met de specifieke toestemming van beheerders en commerciële contactpersonen, waardoor het risico op tijdverlies en ergernis als gevolg van ongevraagde e-mail wordt voorkomen. Nextcloud is ook gestopt met het gebruik van een trackingpixel in zijn nieuwsbrieven.

Al met al leidt de waargenomen verwerking van de account-, diagnostische, ondersteunings- en websitegegevens door Nextcloud, evenals de beslissingen van Nextcloud in de software met betrekking tot de verwerking van diagnostische en websitegegevens, tot **15 lage of beperkte risico's op het gebied van gegevensbescherming**. Op basis van de aangepaste nieuwe DPA met SURF en andere maatregelen die Nextcloud heeft genomen of zal nemen, zijn al deze risico's beperkt, kunnen ze door de onderwijsinstellingen worden beperkt, of zullen ze binnenkort door Nextcloud worden beperkt (uiterlijk eind 2026).

## C.2 Beoordeling van risico's

### C.2.1 Verlies van controle over de verwerking van beheerdersaccountgegevens in Accountgegevens, Diagnostische gegevens, Meta-Ondersteuningsgegevens, en Websitegegevens

Zoals beschreven in [paragraaf A.3.2](#) maakte Nextcloud geen onderscheid tussen beheerdersaccountgegevens en commerciële contactgegevens. Nextcloud beschouwde zichzelf als verwerkingsverantwoordelijke voor beide soorten contactgegevens en inloggegevens. Als verwerkingsverantwoordelijke stond Nextcloud zichzelf toe deze gecombineerde gegevens voor eigen doeleinden te verwerken.

Aangezien de onderwijsinstellingen Nextcloud feitelijk in staat stellen de beheerdersaccountgegevens te verwerken, en de beheerders geen andere keuze hebben dan in te loggen op het beheerders- en het ondersteuningsportaal om hun taken uit te voeren, is de gegevensverwerking door Nextcloud onlosmakelijk verbonden met de verwerking waarvoor de onderwijsinstellingen de Nextcloud Enterprise-software willen gebruiken. Daarom was Nextcloud, zoals betoogd in [paragraaf A.7.4](#), geen onafhankelijke verwerkingsverantwoordelijke voor deze gegevensverwerking, maar een gezamenlijke verwerkingsverantwoordelijke (of op zijn minst een derde partij vanuit het perspectief van de onderwijsinstelling). Onderwijsinstellingen hebben geen rechtsgrond om beheerdersaccountgegevens aan een derde partij bekend te maken. Zonder uitdrukkelijke toestemming van de onderwijsinstellingen zou de verdere verwerking door Nextcloud als verwerkingsverantwoordelijke niet verenigbaar zijn met de doeleinden van de verwerker.

SURF en Nextcloud zijn een limitatieve lijst van verwerkingsdoeleinden overeengekomen, evenals een limitatieve lijst van toegestane doeleinden voor verdere verwerking. Nextcloud is een verwerker van beheerdersaccountgegevens (ook wanneer deze zijn opgenomen in de diagnostische, ondersteunings- en websitegegevens met beperkte toegang). [Paragraaf B.2.4](#) beoordeelt dat de toegestane verdere verwerking van de geaggregeerde beheerdersaccountgegevens ter naleving van wettelijke verplichtingen, en in statistische vorm voor interne rapportage, financiële rapportage en productstrategie, alsmede om de prestaties en efficiëntie van de software technisch te verbeteren en te optimaliseren, verenigbaar is met de overeengekomen doeleinden van de verwerker.

Aangezien beheerdersaccountgegevens gevoelig zijn vanwege de toegang tot diverse persoonsgegevens van eindgebruikers, zoals beschreven in [paragraaf A.2.2.2](#), zou de impact van onverenigbare verdere verwerking groot zijn. Op basis van de gewijzigde DPA heeft Nextcloud de kans op het optreden hiervan echter tot bijna nul teruggebracht. Daarom kan dit risico als opgelost worden aangemerkt.

### **C.2.2 Verlies van controle bij de doorgifte van e-mailadressen naar de VS**

Zoals beschreven in [paragraaf A.7.2.2](#) heeft Nextcloud, in zijn hoedanigheid van verwerkingsverantwoordelijke, besloten een e-mailverzender uit de VS (ActiveCampaign, merknaam Postmark) in te schakelen als verwerker voor al zijn uitgaande e-mail. Zoals geanalyseerd in [paragraaf A.9.1](#) leidt dit tot een gegevensoverdracht naar de VS van de accountgegevens van beheerders en commerciële contactgegevens die automatisch zijn aangemeld voor nieuwsbrieven, evenals de inhoud van de uitgaande e-mail (die 45 dagen in een logbestand wordt bewaard). Hoewel het besluit van de Europese Commissie dat de VS een adequaat niveau van gegevensbescherming bieden formeel nog steeds geldig is, beschouwt SURF digitale soevereiniteit als noodzakelijk om waarden als privacy, autonomie en inclusie te handhaven en te beschermen, zoals beschreven in [paragraaf A.8.1](#).<sup>4</sup> Nextcloud positioneert zich ook als de beste partner voor EU-gegevenssoevereiniteit, zoals beschreven in [paragraaf A.8.2](#).

Een mogelijke openbaarmaking door ActiveCampaign/Postmark van de twee soorten contactgegevens van Nederlandse onderwijsinstellingen aan overheidsinstanties in de VS zou grote gevolgen kunnen hebben, met name als beheerdersaccountgegevens vervolgens

---

<sup>4</sup> Idem.

worden gebruikt voor spear-phishing, om toegang te krijgen tot meer gegevens die zijn opgeslagen in de Nextcloud Enterprise-software. In reactie op de bezorgdheid van SURF over deze gegevensoverdracht heeft Nextcloud zich er echter toe verbonden om in het derde kwartaal van 2026 over te stappen op een e-mailprovider die binnen de EU is gevestigd. Zodra deze overstap is voltooid, is de kans op ongeoorloofde toegang door overheidsinstanties in de VS nihil, aangezien Nextcloud ook contractueel met SURF is overeengekomen om verzoeken van niet-EU-instanties altijd af te wijzen. Daarom kan dit risico tegen het derde kwartaal van 2026 als laag worden aangemerkt.

Bovendien zullen beheerders van onderwijsinstellingen regelmatig de in de VS gevestigde en gehoste repository GitHub moeten bezoeken voor beveiligingsadviezen van Nextcloud en om updates te downloaden, en mogelijk ook Hugging Face om de Whisper LLM te downloaden als onderdeel van de geteste generatieve AI-transcriptieoplossing Talk. Om het risico op gedwongen openbaarmaking aan Amerikaanse overheidsinstanties door deze twee derde partijen te beperken, moeten beheerders voorkomen dat hun privé-IP-adressen en persoonlijke apparaatgegevens worden gedeeld wanneer ze deze bronnen raadplegen, bijvoorbeeld door een VPN te gebruiken en/of cookies en lokale opslag te wissen, en het lekken van een apparaatvingerafdruk te voorkomen. Bovenal mogen beheerders niet permanent ingelogd blijven op GitHub en Hugging Face.

### **C.2.3 Verlies van controle bij doorgifte van Ondersteuningsgegevens naar Collabora buiten de EU**

In de testopstelling voor deze DPIA gebruikte SURF Nextcloud Office als kantoor suite. Nextcloud biedt ook ondersteunde toegang tot andere suites voor het bewerken van kantoordocumenten, van ONLYOFFICE, ThinkFree Office en de on-premises versie van Microsoft Office.<sup>5</sup>

Zoals beschreven in paragraaf A.1.2.1 is Nextcloud Office een frontend voor de Collabora Online-software van het Britse bedrijf Collabora. Als een onderwijsinstelling Nextcloud om ondersteuning vraagt met betrekking tot Nextcloud Office, is het ticket toegankelijk voor medewerkers van het bedrijf Collabora. Zoals beschreven in paragraaf A.9.1 heeft Nextcloud op verzoek van SURF ervoor gezorgd dat de toegang voor medewerkers van Collabora tot de relevante supporttickets in Zammad beperkt is tot medewerkers die zich fysiek in de EU en het Verenigd Koninkrijk bevinden. Nextcloud heeft toegezegd de toegang te beperken tot medewerkers die in de EU zijn gevestigd, mocht het adequaatheidsbesluit voor het Verenigd Koninkrijk ongeldig worden. Nextcloud heeft zelf ook medewerkers die buiten de EU zijn gevestigd, maar had de toegang technisch al beperkt tot medewerkers die zich fysiek in de EU bevinden (zie Figuur 35).

Een mogelijke ongeoorloofde openbaarmaking van ondersteuningsgesprekken en metadata aan overheidsinstanties buiten de EU, waar medewerkers van Collabora gevestigd zijn, zou ernstige gevolgen kunnen hebben, indien die informatie vervolgens kan worden gebruikt om een beheerder te (spear-)phishen of op een andere manier de integriteit van de software aan te tasten. Dankzij deze twee risicobeperkende maatregelen heeft Nextcloud de kans dat dit zich voordoet echter tot bijna nul teruggebracht. Daarom kan dit risico als opgelost worden beschouwd.

---

<sup>5</sup> Antwoord van Nextcloud op deel A van deze DPIA, 2 april 2026.

#### **C.2.4 Verlies van vertrouwelijkheid door het ontbreken van 2FA op het ondersteuningsportaal**

Zoals beschreven in de beveiligingsbeoordeling in [paragraaf A.6.1](#) biedt Nextcloud een beheerders- en een ondersteuningsportaal aan via een website die wordt onderhouden door zijn (Duitse) subverwerker Zammad. Nextcloud vereist nog geen tweefactorauthenticatie om in te loggen. Zonder deze maatregel is het voor kwaadwillende actoren gemakkelijker om toegang te krijgen tot deze pagina's met beperkte toegang en beheerdersaccounts te compromitteren.

Nextcloud heeft samen met Zammad aan een oplossing voor dit probleem gewerkt en heeft toegezegd om 2FA af te dwingen op het beheerders- en ondersteuningsportaal in de nieuwe versie v7.1 van het ondersteuningsportaal van Zammad, die op 1 juli 2026 is uitgebracht. Hoewel de impact van inbreuken op beheerdersaccounts groot kan zijn, heeft Nextcloud de kans dat dit gebeurt effectief tot een laag niveau teruggebracht. Zodra Nextcloud de tests heeft afgerond en de nieuwe portaalversie uitbrengt, is het risico verholpen.

Opmerking: om organisaties te helpen die besluiten de Nextcloud Enterprise-software zelf te hosten, heeft SURF een voorlopige tabel met noodzakelijke beveiligingsmaatregelen opgesteld in [paragraaf C.1.1.1](#).

#### **C.2.5 Verlies van controle door gebrek aan transparantie: Diagnostische gegevens**

Hoewel de Nextcloud Enterprise-software is ontworpen om klanten in staat te stellen de gegevensverwerking zelf te beheren en te controleren, blijkt uit de technische analyse van netwerkverkeersgegevens, zoals beschreven in [paragraaf A.3.3](#), dat het bedrijf Nextcloud GmbH optioneel drie soorten diagnostische gegevens van beheerders kan verzamelen en verwerken: via de gebruiksenquête, het systeem-informatierapport en gegevens die automatisch worden gedeeld via de support-app.

De logbestanden bevatten gepseudonimiseerde gegevens zoals unieke klant- (organisatie-) of apparaat-ID's, en/of IP-adressen die betrekking hebben op een specifieke organisatie, plus configuratiegegevens of statistieken over het aantal gebruikers (identificeerbaar voor de onderwijsinstellingen). Aangezien Nextcloud ook over accountgegevens van beheerders en commerciële contactgegevens beschikt, is Nextcloud technisch in staat om deze gegevens te koppelen aan identificeerbare personen binnen de klantorganisaties. Nextcloud verstrekt geen openbare documentatie over de inhoud van deze logbestanden.

Op basis van de gewijzigde DPA met SURF is Nextcloud verwerker geworden voor deze diagnostische gegevens en zal het deze gegevens alleen in identificeerbare vorm verwerken voor de vier overeengekomen doeleinden. Nextcloud heeft ook de keuze voor beheerders verbeterd om al dan niet de gegevens uit de gebruiksenquête te delen. Om de gegevensstroom naar Nextcloud verder te minimaliseren, kunnen onderwijsinstellingen het gebruik van gepseudonimiseerde beheerdersaccounts overwegen, bijvoorbeeld door middel van identiteitsfederatie, wanneer zij besluiten dat zij gegevens uit de gebruiksenquête met Nextcloud willen delen.

Zoals beschreven in [paragraaf A.11.2](#) heeft Nextcloud zich ertoe verbonden de verwerking van diagnostische gegevens (gebruiksonderzoek, systeem-informatierapport en gegevens

van de ondersteuningsapp) te documenteren en vastgestelde bewaartermijnen voor deze gegevens te publiceren. De gewijzigde DPA bevat ook de bewaartermijnen van deze drie rapporten met identificeerbare gegevens.

Vóór de onderhandelde DPA waren de bewaartermijnen van deze logbestanden onbekend. Hoe langer gegevens worden bewaard, hoe groter de potentiële impact in geval van ongeoorloofde toegang. Op basis van de gewijzigde DPA en de toezegging van Nextcloud om deze bewaartermijnen openbaar te maken, is de kans op verlies van controle echter zeer klein. Daarom kan dit risico als laag worden aangemerkt.

### **C.2.6 Verlies van controle door gebrek aan transparantie en risico op heridentificatie van andere Diagnostische gegevens, activiteitenlogboeken van het ondersteuningssysteem en Websitegegevens**

Naast de drie soorten diagnostische gegevens die Nextcloud via beheerders verzamelt (zie [paragraaf C.2.5](#) hierboven), kan Nextcloud op afstand zeven soorten logbestanden met persoonsgegevens aanmaken die niet toegankelijk zijn voor beheerders (zie [paragraaf A.3.3.3](#)):

1. Logboek voor het downloaden en updaten van software
2. Logboek van de proxy voor pushmeldingen
3. Activiteitenlogboek in het supportticketsysteem van Zammad
4. Toegangslogboek van de webserver (bezoeken aan de Support Hub-website met beperkte toegang, aan portal.nextcloud.com en aan de openbaar toegankelijke website nextcloud.com van Nextcloud)
5. Logboek van uitgaande e-mails naar klanten, inclusief nieuwsbrieven (via ActiveCampaign / Postmark)
6. Logboek van licentieverdeling (via Sendent, uitsluitend in dit specifieke testscenario<sup>6</sup>)
7. Logboek van privacy- en toegangsverzoeken (via DataCo)

Nextcloud biedt geen openbare documentatie over de inhoud van deze logbestanden. Nextcloud heeft SURF aanvullende informatie verstrekt en heeft toegezegd informatie te publiceren over de verwerking van deze zeven logbestanden, inclusief de bewaartermijnen. SURF heeft deze documentatie beoordeeld en is van mening dat dit het gebrek aan transparantie op adequate wijze verhelpt.

Op het portaal met beperkte toegang en de ondersteuningspagina's plaatst Nextcloud standaard alleen functionele cookies (geen analytische cookies), maar documenteert deze cookies niet. Zoals te zien is in [Tabel 7](#), bewaart Nextcloud het toegangslogboek van de webserver slechts zeven dagen en slaat het de cookiegegevens niet op buiten de browser van de eindgebruiker.

Om de kans op controleverlies verder te verkleinen, zijn SURF en Nextcloud overeengekomen dat Nextcloud in het algemeen optreedt als verwerker voor deze zeven logbestanden, met uitzondering van het logbestand van uitgaande e-mail naar commerciële

---

<sup>6</sup> In antwoord op vragen van SURF over de gegevensverwerking door Sendent legde Nextcloud uit: „Dit is geen standaardinstelling. Sendent ontwikkelt optionele componenten die op verzoek kunnen worden aangeschaft. Als u Nextcloud Enterprise in het Ultimate-abonnement aanschaft, zijn hun producten inbegrepen en worden deze dus naast onze licentie geleverd.” Antwoord van Nextcloud van 6 mei 2026. Om SURF één Enterprise-testlicentie te verstrekken, maakte Nextcloud ook gebruik van Sendent.

contactgegevens (waarbij Nextcloud optreedt als geautoriseerde verwerkingsverantwoordelijke). Namens de onderwijsinstellingen kan SURF het recht uitoefenen om te controleren of Nextcloud voldoet aan de bepalingen in de gewijzigde DPA. Dit controlerecht omvat zowel de verwerking door Nextcloud als verwerker als de verwerking door Nextcloud als geautoriseerde verwerkingsverantwoordelijke.

In reactie op de technische bevindingen inzake cookies heeft Nextcloud de cookie-informatie op zijn openbare website bijgewerkt en een fout gecorrigeerd. Onderwijsinstellingen dienen beheerders te instrueren de standaard privacyvriendelijke cookie-instellingen op de openbare website nextcloud.com niet te wijzigen.

Een gebrek aan transparantie heeft een negatieve invloed op het vermogen van beheerders om hun recht op inzage voor betrokkenen uit te oefenen. Op basis van de nieuwe documentatie van Nextcloud (zoals goedgekeurd door SURF) is de kans op verlies van controle echter zeer klein. Daarom kan dit risico als laag worden aangemerkt.

### **C.2.7 Verlies van controle en gebrek aan transparantie bij subverwerkers**

Zoals beschreven in de feitelijke analyse van de rol van Nextcloud in het kader van de AVG op basis van de openbare contractdocumentatie (paragraaf A.7.2.2) geeft Nextcloud zijn klanten geen controle over de (sub)verwerkers die het inschakelt. Op basis van de gewijzigde DPA met SURF kunnen Nederlandse onderwijsinstellingen deze controle echter uitoefenen via een aantal contractuele maatregelen. Nextcloud verbindt zich ertoe uitsluitend subverwerkers in te schakelen die persoonsgegevens binnen de EU verwerken, met twee tijdelijke uitzonderingen (de Amerikaanse e-maildienstverlener en medewerkers van Collabora in het Verenigd Koninkrijk). De gewijzigde DPA met SURF waarborgt tevens dat Nextcloud de onderwijsinstellingen 60 werkdagen van tevoren (behalve in noodsituaties) op de hoogte stelt voordat nieuwe subverwerkers worden ingeschakeld.<sup>7</sup>

Hoewel de gevolgen van het inschakelen van ongeautoriseerde (sub)verwerkers groot zouden kunnen zijn, heeft Nextcloud de kans hierop effectief tot bijna nul teruggebracht. Dit risico is derhalve opgelost.

### **C.2.8 Onvermogen om betrokkenrechten uit te voeren**

Zoals beschreven in paragraaf A.3.6 en beoordeeld in paragraaf B.6.2, heeft Nextcloud snel en gedetailleerd gereageerd op de verzoeken om inzage (DSAR's) die door SURF waren ingediend. Het antwoord was echter niet altijd correct (er werd verzuimd de Nederlandse gegevensbeschermingsautoriteit te vermelden), maar wat nog belangrijker is: het was niet volledig. Nextcloud heeft de toegang tot persoonsgegevens niet expliciet geweigerd en stemde ermee in om, voor zover mogelijk, volledige toegang te verlenen tot alle beschikbare persoonsgegevens die het verwerkt als verwerker en als geautoriseerde verwerkingsverantwoordelijke, mits de gegevens nog beschikbaar zijn en/of de betrokkene de juiste identificatiegegevens kan verstrekken zodat Nextcloud de gegevens kan opvragen.

De gevolgen van een ongerechtvaardigde weigering om toegang te verlenen zouden zeer groot zijn, aangezien het recht op inzage van de betrokkene deze in staat stelt de rechtmatigheid van de gegevensverwerking te begrijpen en op basis van het antwoord

---

<sup>7</sup> Nextcloud DPA-sjabloon, paragraaf 7.7, Gebruik van subverwerkers.

andere rechten uit te oefenen, zoals het recht om te verzoeken om verwijdering van persoonsgegevens. Gezien de toezegging van Nextcloud om volledige toegang te verlenen tot alle beschikbare persoonsgegevens, is de waarschijnlijkheid dat dit zich voordoet echter vrijwel nul. Daarom kan het risico als laag worden aangemerkt.

#### **C.2.9 Onvermogen om het recht van de betrokkene op verwijdering van Ondersteuningsgegevens uit te oefenen**

De gebruikersinterface van het Supportportaal van Nextcloud biedt beheerders geen mogelijkheden om individuele of meerdere supporttickets of bijlagen te verwijderen. Zoals beschreven in [paragraaf A.3.4](#) en beoordeeld in [paragraaf B.5.1.3](#), bewaarde Nextcloud gesloten supporttickets aanvankelijk gedurende 4 jaar. Als verwerker is het niet aan Nextcloud om deze bewaartermijn vast te stellen, maar aan de verwerkingsverantwoordelijke, de onderwijsinstelling. In het algemeen moeten organisaties motiveren waarom zij tickets met identificeerbare gegevens langer dan 13 maanden moeten bewaren (voldoende om jaarlijks terugkerende incidenten vast te leggen). Op basis van de gewijzigde verwerkersovereenkomst met SURF mag Nextcloud gepseudonimiseerde, geaggregeerde supporttickets zo lang als nodig gebruiken om te leren van ervaringen uit het verleden en de software en diensten te blijven verbeteren, maar deze instructie is niet van toepassing op de direct identificeerbare gegevens.

Nextcloud heeft ermee ingestemd om de bewaartermijn voor SURF-leden te verkorten tot 15 maanden, en klanten kunnen Nextcloud vragen om afzonderlijke tickets en bijlagen of alle tickets te verwijderen voordat deze verkorte bewaartermijn is verstreken. Nextcloud heeft op [portal.nextcloud.com](https://portal.nextcloud.com) al een waarschuwing voor beheerders toegevoegd om geen persoonsgegevens in bijlagen te uploaden, en Nextcloud is met Zammad overeengekomen om in het derde kwartaal van 2026 dezelfde waarschuwing op [support.nextcloud.com](https://support.nextcloud.com) te implementeren.

Hoewel het onvermogen om het recht op verwijdering uit te oefenen formeel als een zeer hoog risico wordt aangemerkt, verlagen de verkorte bewaartermijn, de waarschuwingen en de mogelijkheid om Nextcloud te vragen tickets te verwijderen samen – gezien het belang dat de AVG hecht aan de uitoefening van grondrechten – de kans dat het risico van het onvermogen om persoonsgegevens te verwijderen zich voordoet tot een verwaarloosbaar niveau. Daarom kan dit risico als laag worden aangemerkt.

#### **C.2.10 Verlies van controle over de openbaarmaking van (beperkte) persoonsgegevens aan overheidsinstanties binnen en buiten de EU**

Nextcloud GmbH verzamelt beperkte hoeveelheden persoonsgegevens. En als Duits bedrijf dat volledig in Duitse handen is, is Nextcloud GmbH niet rechtstreeks onderworpen aan Amerikaanse of andere niet-EU-wetgeving. Deze omstandigheden maken het op zich al onwaarschijnlijk dat Nextcloud GmbH door overheidsinstanties buiten de EU zou kunnen worden gedwongen om persoonsgegevens met betrekking tot Nederlandse klanten in het onderwijs openbaar te maken. Nextcloud heeft bevestigd dat het nog nooit een verzoek tot openbaarmaking heeft ontvangen.

Het bedrijf verkoopt zijn software echter wel aan klanten buiten de EU. Zoals beschreven in [paragraaf A.5.2.2](#) (doel van naleving van wettelijke verplichtingen) bestaat er een (theoretisch) risico dat Nextcloud GmbH gedwongen (gechanteerd) zou kunnen worden om

de levering van de software aan één of alle EU-kanten te staken. De Amerikaanse overheid zou het gehele bedrijf Nextcloud GmbH op een van haar sanctielijsten kunnen plaatsen indien het diensten zou blijven verlenen aan een gesanctioneerde persoon of organisatie in de VS of elders. Een dergelijke sanctie zou Amerikaanse klanten verbieden Nextcloud Enterprise-diensten aan te schaffen, en zou Nextcloud daarmee economisch chanteren in overeenstemming met extraterritoriale wetgeving. Nextcloud antwoordde dat dit soort chantage niet zou werken, aangezien Amerikaanse klanten slechts een klein deel van de omzet uitmaken en het een verstandige zakelijke beslissing zou zijn om de activiteiten in de VS te staken.

Om de lage waarschijnlijkheid dat dit risico zich voordoet nog verder te onderstrepen, heeft Nextcloud ingestemd met vier contractuele maatregelen/toezeggingen in de gewijzigde DPA met SURF:

1. Nextcloud zal verzoeken van autoriteiten buiten de EU onvoorwaardelijk afwijzen.
2. Nextcloud zal de gegevens die het gedwongen kan worden aan EU-autoriteiten te verstrekken, tot een minimum beperken. Nextcloud zal elk verzoek grondig juridisch toetsen indien het verboden is het verzoek door te sturen naar de klant, en zal uit principe bezwaar maken tegen het verzoek.
3. Nextcloud zal jaarlijks transparantiestatistieken publiceren over het aantal verzoeken en het aantal keren dat gegevens zijn verstrekt.
4. Nextcloud heeft niet opzettelijk „achterdeurtjes“ of soortgelijke programmering in de software aangebracht die door derden zou kunnen worden gebruikt om toegang te krijgen tot het systeem en/of persoonsgegevens, noch heeft het zijn bedrijfsprocessen gewijzigd, noch is het onderworpen aan enige wetgeving die het zou verplichten achterdeurtjes in te voeren.

Deze toezeggingen verlagen de kans op het optreden van dergelijke situaties verder tot bijna nul. Hoewel de impact van een mogelijke openbaarmaking aan autoriteiten buiten de EU groot kan zijn, kan het risico als laag worden aangemerkt.

### **C.2.11 Verlies van controle over verwerkingen van Nextcloud als onafhankelijke verwerkingsverantwoordelijke**

Vóór de gewijzigde verwerkersovereenkomst (DPA) met SURF beschouwde Nextcloud zichzelf als een onafhankelijke verwerkingsverantwoordelijke voor alle gegevensverwerking, met uitzondering van de inhoud van supporttickets. Zoals geanalyseerd in [paragraaf A.7.4](#) viel de gegevensverwerking onder het privacy- en juridisch beleid van Nextcloud.

Op grond van artikel 28, lid 10, van de AVG worden verwerkers die zelf beslissingen nemen over de doeleinden van de verwerking, onrechtmatig verwerkingsverantwoordelijken. Nextcloud kon echter niet worden aangemerkt als onafhankelijke verwerkingsverantwoordelijke, maar moest worden aangemerkt als een de facto gezamenlijke verwerkingsverantwoordelijke met de klant die de verwerking mogelijk maakt door gebruik te maken van de Nextcloud Enterprise-software.

Noch SURF, noch Nextcloud wilden een overeenkomst inzake gezamenlijke verwerkingsverantwoordelijkheid aangaan om de doeleinden van de verwerking en de uitoefening van de rechten van betrokkenen te specificeren. In plaats daarvan stemde

Nextcloud ermee in om een limitatieve lijst van zeven toegestane doeleinden voor verdere verwerking op te nemen in de DPA. Zoals uiteengezet in [paragraaf B.2.4](#) heeft SURF beoordeeld dat verdere verwerking voor deze doeleinden verenigbaar is met de oorspronkelijke doeleinden van de gegevensverzameling. Daarnaast heeft Nextcloud ermee ingestemd de accountgegevens van beheerders te scheiden van de commerciële contactgegevens, om verwarring te voorkomen over de rol van Nextcloud als verwerker van de contactgegevens van beheerders en de rol van Nextcloud als geautoriseerde verwerkingsverantwoordelijke voor de commerciële contactgegevens.

Hoewel Nextcloud in zijn hoedanigheid als verwerkingsverantwoordelijke in zijn privacy- en juridisch beleid geen melding maakt van doeleinden van de gegevensverwerking die een hoog risico inhouden, moest de impact van ongeoorloofde verdere verwerking van de beheerdersaccount-, ondersteunings- en diagnostische gegevens voor eigen doeleinden van Nextcloud toch als gemiddeld worden beoordeeld. Op basis van de gewijzigde verwerkersovereenkomst (DPA) met SURF, inclusief de afspraak over de standaard privacy-instellingen van de openbare website, is de kans op verlies van controle over de doeleinden van de verwerkingsverantwoordelijke echter vrijwel nihil. Daarom kan dit risico als opgelost worden aangemerkt.

#### **C.2.12 Verlies van controle: gebruik van trackingpixel in uitgaande e-mail van Nextcloud**

Zoals beschreven in [paragraaf A.10](#) heeft Nextcloud een trackingpixel toegevoegd aan alle uitgaande e-mail. Met behulp van deze onzichtbare 1x1-pixels verzamelde Nextcloud interactiegegevens, zoals het lezen, openen of aanklikken van zijn nieuwsbrieven.

Nextcloud heeft deze gegevensverwerking niet gedocumenteerd, noch heeft het gebruikers om toestemming gevraagd. In navolging van eerder advies van de gegevensbeschermingsautoriteiten in de EU, verenigd in de Artikel 29-werkgroep, heeft het EDPB ook toegelicht dat het gebruik van trackingpixels onder het toepassingsgebied van artikel 5, lid 3, van de e-privacyrichtlijn valt. Daarom is voorafgaande geïnformeerde toestemming vereist, evenals een mogelijkheid om de gegevensverwerking te weigeren.

Het gebrek aan transparantie maakte deze verwerking inherent oneerlijk, zoals beoordeeld in [paragraaf B.5.1.1](#). Deze ondoorzichtige verwerking had een beperkte impact, aangezien het toezicht alleen betrekking had op zakelijke communicatie, maar de impact van heimelijk toezicht kan niet als verwaarloosbaar worden beschouwd. Om dit risico te beperken, konden onderwijsinstellingen beheerders alleen aanbevelen om het downloaden van afbeeldingen in hun webmail uit te schakelen, maar een dergelijke organisatorische maatregel is veel minder effectief dan een technische maatregel.

In reactie op deze analyse heeft Nextcloud de trackingpixel echter uitgeschakeld. Hierdoor wordt de kans dat beheerders hun leesgedrag prijsgeven tot nul teruggebracht. Ook de impact wordt tot nul teruggebracht. Dit risico is daarmee opgelost.

#### **C.2.13 Verlies van controle over gegevens van beheerdersaccounts in nieuwsbrieven**

Vóór de onderhandelingen over een gewijzigde DPA met SURF beschouwde Nextcloud zichzelf als een onafhankelijke verwerkingsverantwoordelijke voor de beheerdersaccountgegevens die het verzamelt, samen met de commerciële

contactgegevens, of wanneer men zich abonneert op een of meer nieuwsbrieven. Zoals beoordeeld in [paragraaf C.2.1](#) zijn beheerdersaccountgegevens gevoelig vanuit het perspectief van hun toegang tot meerdere persoonsgegevens van eindgebruikers. Zoals beschreven in [paragraaf A.2.2.2](#) zou de impact van onverenigbare verdere verwerking groot zijn.

Om te voorkomen dat het risico ontstaat dat de controle over deze beheerdersaccountgegevens verloren gaat, heeft Nextcloud ingestemd met twee technische maatregelen: het duidelijk onderscheiden van de beheerdersaccountgegevens en de commerciële contactgegevens, en het opzetten van een doe-het-zelfportaal voor het aan- en afmelden voor nieuwsbrieven, beide in het derde kwartaal van 2026.

Gezien deze maatregelen kan de waarschijnlijkheid worden teruggebracht tot „zeer klein“ en kan het risico als „laag“ worden aangemerkt.

#### **C.2.14 Verlies van controle door gebrek aan transparantie over het bestaan van meerdere logbestanden in de software**

Nextcloud genereerde veel verschillende logbestanden in de zelfgehoste software. Toegang tot deze logbestanden is essentieel voor organisaties om te voldoen aan beveiligingsverplichtingen en om te controleren op gegevenslekken of het opsporen van afwijkende activiteiten. Daarnaast moeten organisaties buitensporige bewaartermijnen voor gegevens voorkomen. De inhoud van de audit- en interactielogbestanden met persoonsgegevens, zoals geanalyseerd door SURF, is toereikend (zie [paragraaf A.3.3.1.1](#)), maar SURF constateerde de aanwezigheid van ten minste 14 andere logbestanden (zie de lijst aan het einde van [paragraaf A.3.3](#)). De beschikbaarheid, inhoud en standaardbewaartermijnen van deze logbestanden zijn onvoldoende gedocumenteerd.

Nextcloud heeft toegezegd om in het derde kwartaal van 2026 centrale informatie te publiceren over het bestaan van de verschillende logbestanden voor beheerders, en om beter uit te leggen wanneer Nextcloud-logbestanden gevoelige en identificeerbare informatie kunnen vastleggen in de audit- en chatlogbestanden.

Onderwijsinstellingen kunnen deze DPIA nu al gebruiken om beheerders te informeren en hun Register van Verwerkingsactiviteiten (ROPA) bij te werken, en zullen binnenkort ook gebruik kunnen maken van nieuwe centrale documentatie van Nextcloud. De gevolgen van een gebrek aan transparantie kunnen niet te verwaarlozen zijn, aangezien sommige logbestanden mogelijk te kort worden bewaard om afwijkingen op te sporen – met name als een datalek onopgemerkt blijft – terwijl andere logbestanden juist te lang worden bewaard. De toezegging van Nextcloud verkleint de kans dat toekomstige klanten niet op de hoogte zijn van het bestaan en de bewaartermijn van logbestanden op afstand. Daarom kan dit risico als laag worden aangemerkt.

#### **C.2.15 Chilling effect: monitoringsysteem voor medewerkers en studenten**

Onderwijsinstellingen hebben in hun zelfgehoste software toegang tot audit- en interactielogbestanden met informatie over de specifieke acties en documenten die door eindgebruikers zijn geraadpleegd, en inlogpatronen, zoals beschreven in [paragraaf A.3.3.1.1](#). De logbestanden bevatten direct en indirect identificeerbare gegevens. Sommige

van deze logbestanden bevatten inhoudelijke gegevens, zoals bestandsnamen of namen van (verwijderde) vergaderruimten.

Op basis van deze logbestanden kunnen beheerders het individuele werk- en studiegedrag volgen. Als onderwijsinstellingen deze diagnostische gegevens zouden gebruiken als systeem voor het monitoren van medewerkers en/of studenten, zouden de gevolgen zeer ingrijpend kunnen zijn. Het besef dat een werkgever gedetailleerde gebruiksgegevens kan verwerken voor evaluatiedoeleinden, kan een *afschrikkend effect* hebben op docenten en studenten die de Nextcloud Enterprise-software gebruiken. Zij kunnen vrezen dat de monitoring wordt gebruikt voor een negatieve prestatiebeoordeling, tenzij dit specifiek is uitgesloten in een (intern) privacybeleid voor de verwerking van persoonsgegevens van medewerkers en studenten. Dergelijke monitoring kan hen beletten legitiem gebruik te maken van daarmee samenhangende grondrechten, zoals de vrijheid om informatie te verzenden en te ontvangen.

Om organisaties te helpen dit risico te voorkomen, heeft Nextcloud toegezegd om tegen eind 2026 een tweede export van de audit- en interactielogboeken te maken, waarin de gebruikersnamen en inhoudelijke gegevens worden gemaskeerd met \*\*\*. Organisaties kunnen deze geredigeerde logboeken importeren in hun eigen logboekbeheersysteem. Deze oplossing biedt een evenwicht tussen de noodzaak van onveranderlijke auditlogboeken om alle activiteiten vast te leggen – inclusief pogingen tot het wissen van kwaadwillige activiteiten – en de verplichting op grond van de AVG om de risico's voor betrokkenen van buitensporige, onnodige gegevensverwerking tot een minimum te beperken.

In de context van de Nederlandse onderwijssector is de kans dat deze gegevensverwerking tot afschrikkende effecten leidt, zeer klein. Deze DPIA gaat ervan uit dat onderwijsinstellingen de aanbeveling opvolgen om de toegang tot de onbewerkte audit- en interactielogboeken tot het absolute minimum te beperken, en alleen de bewerkte logboeken gebruiken voor het dagelijkse softwarebeheer en de beveiligingsmonitoring.

Bovendien gaat deze DPIA ervan uit dat onderwijsinstellingen een intern privacybeleid zullen implementeren met regels en legitieme, specifieke doeleinden voor de (verdere) verwerking van de logbestanden met de ruwe gegevens, inclusief toezicht op de toegang van (globale/root-)beheerders tot deze ruwe gegevens.

Ervan uitgaande dat onderwijsinstellingen een adequaat intern privacybeleid implementeren en de naleving daarvan controleren, kunnen de risico's voor betrokkenen als laag worden aangemerkt.

Tabel3 : Beoordeling van de 15 geïdentificeerde risico's

| Ernst van de gevolgen | Ernstige schade | Laag risico<br>1, 2, 3, 4, 5, 6, 7,<br>8, 9, 10, 11, 13,<br>15 | Hoog risico | Hoog risico |
|-----------------------|-----------------|----------------------------------------------------------------|-------------|-------------|
|                       |                 |                                                                |             |             |

|  |                                           |                       |                     |                              |
|--|-------------------------------------------|-----------------------|---------------------|------------------------------|
|  | Enige impact                              | Laag risico<br>12, 14 | Gemiddeld<br>risico | Hoog risico                  |
|  | Minimale impact                           | Laag risico           | Laag risico         | Laag risico                  |
|  |                                           | Op afstand            | Redelijke kans      | Waarschijnlijker<br>dan niet |
|  | Waarschijnlijkheid van schade (voorkomen) |                       |                     |                              |

## Part D Beschrijving van de voorgestelde risicobeperkende maatregelen

### D.1 Beperkende maatregelen

Het volgende gedeelte bevat een tabel met de technische, organisatorische en juridische maatregelen die door Nextcloud en door de onderwijsinstellingen (inclusief de aanbieder van hun volledig beheerde oplossing) moeten worden genomen of al zijn genomen om de 15 geïdentificeerde gegevensbeschermingsrisico's te beperken.

#### D.1.1 Voorgestelde en genomen maatregelen om risico's te beperken

Deze tabel geeft een overzicht van de aanbevolen maatregelen voor onderwijsinstellingen, de aanbevolen maatregelen voor Nextcloud en de maatregelen die Nextcloud heeft genomen of toegezegd als gevolg van het nieuwe contract met SURF.

Mits de onderwijsinstellingen de aanbevolen maatregelen implementeren, worden alle 15 geïdentificeerde risico's gemitigeerd (opgelost in de tabel) of kunnen ze worden teruggebracht tot een laag risico.

Tabel4 : Overzicht van gegevensbeschermingsrisico's, risicobeperkende maatregelen en restrisico's

| Aantal | Risico's                                                                                                                                                       | Aanbevolen maatregelen voor onderwijsinstellingen                                                                                                                                   | Maatregelen die door NEXTCLOUD zijn genomen of toegezegd                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Resterende risico's |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| 1      | Verlies van controle over de verwerking van beheersaccountgegevens in Accountgegevens, Diagnostische gegevens, Meta-Ordersteuningsgegevens, en Websitegegevens | Meld je aan voor Nextcloud Enterprise via SURF, en zorg er bij aanmelding via een reseller of aanbieder van een volledig beheerde oplossing voor dat de SURF-DPA van toepassing is. | <p>Overeenstemming bereikt over beperkende lijst van vier verwerkingsdoeleinden in de gewijzigde DPA.</p> <p>Overeenstemming bereikt over een limitatieve lijst van zeven toegestane doeleinden voor verdere verwerking (legitieme bedrijfsactiviteiten) in de gewijzigde DPA.</p> <p>Overeenstemming bereikt over drie expliciete verwerkingsverboden: geen verdere verwerking voor andere doeleinden, geen verwerking voor reclamadoeleinden of het aanbieden van advertenties, niet voor direct marketing, profilering, onderzoek of analytische doeleinden, tenzij de klant Nextcloud hiertoe opdracht geeft, en geen CSAM-scanning.</p> <p>Er is overeenstemming bereikt over een uitgebreid auditrecht</p> | opgelost            |
|        |                                                                                                                                                                | (SURF): gebruik van het auditrecht om de                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                     |

|    |                                                                                           |                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |          |
|----|-------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|    |                                                                                           | naleving van de doelbinding, gegevensminimalisatie en bewaartermijnen te controleren.                                                                                                                                                                                        | <p>voor SURF namens de onderwijsinstellingen in de gewijzigde DPA.</p> <p>Toezegging gedaan om de beveiligingsaudit voor CSPN om de drie jaar te herhalen en de volledige bevindingen met SURF te delen.</p>                                                                                                                                                                                                                                                                                                       |          |
| 2. | Verlies van controle bij de doorgifte van e-mailadressen naar de VS                       | <p>-</p> <p>Beheerders instrueren om te voorkomen dat zij hun privé-IP-adressen en persoonlijke apparaatgegevens delen bij het gebruik van GitHub en Hugging Face.</p> <p>Geef beheerders de instructie om niet permanent ingelogd te blijven op GitHub en Hugging Face.</p> | <p>Toezegging gedaan om in het derde kwartaal van 2026 over te stappen op een in de EU gevestigde e-mailprovider.</p> <p>Nextcloud verwerkt als verwerker gegevens uitsluitend binnen de EU, zoals overeengekomen in de gewijzigde DPA, met uitzondering van door klanten gekozen subverwerkers buiten de EU, zoals Collabora.</p> <p>Nextcloud zal in het derde kwartaal van 2026 twee soorten abonnementen aanbieden aan Enterprise-klanten: als commercieel contactpersoon voor een klant of als beheerder.</p> | laag     |
| 3. | Verlies van controle bij doorgifte van Ondersteuningsgegevens naar Collabora buiten de EU | -                                                                                                                                                                                                                                                                            | <p>De toegang tot de relevante Collabora-tickets in Zammad is beperkt tot medewerkers die zich fysiek in het Verenigd Koninkrijk en in de EU bevinden.</p> <p>Toezegging gedaan om toegang door medewerkers in het Verenigd Koninkrijk te blokkeren als de adequaatheidsstatus ongeldig wordt.</p>                                                                                                                                                                                                                 | opgelost |
| 4. | Verlies van vertrouwelijkheid door een beveiligingsinbreuk                                | -                                                                                                                                                                                                                                                                            | Nextcloud zal 2FA afdwingen op het beheer- en ondersteuningsportaal in de nieuwe versie v7.1 van het ondersteuningsportaal van Zammad, die op 1 juli 2026 is uitgebracht.                                                                                                                                                                                                                                                                                                                                          | opgelost |
| 5. | Verlies van                                                                               | Optioneel: overweeg het gebruik van                                                                                                                                                                                                                                          | Er is overeengekomen om Diagnostische gegevens op te                                                                                                                                                                                                                                                                                                                                                                                                                                                               | laag     |

|    |                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |      |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
|    | controle door gebrek aan transparantie: Diagnostische gegevens worden optioneel gedeeld door beheerders                                                                                     | <p>gepseudonimiseerde beheerdersaccounts, bijvoorbeeld door middel van identiteitsfederatie om gebruiksonderzoeksgegevens te delen met Nextcloud</p> <p>(SURF): audits uitvoeren op de naleving van doelbinding, gegevensminimalisatie en bewaartermijnen, zowel als verwerker als geautoriseerde verwerkingsverantwoordelijke.</p>                                                                                                                                                                                                      | <p>nemen in de uitgebreide reikwijdte van de gewijzigde DPA.</p> <p>Bewaartermijnen voor 3 soorten logbestanden die optioneel door beheerders worden gedeeld, zijn overeengekomen in de gewijzigde DPA.</p> <p>Deze bewaartermijnen zullen in juli 2026 openbaar worden vastgelegd.</p> <p>Er is overeengekomen dat SURF uitgebreide auditmogelijkheden krijgt in de gewijzigde DPA.</p>                                                           |      |
| 6. | Verlies van controle door gebrek aan transparantie en risico op heridentificatie van andere Diagnostische gegevens, activiteiten-logboeken van het ondersteuningssysteem en Websitegegevens | <p>Beheerders informeren over de functionele cookies via deze overkoepelende DPIA en hen instrueren de standaardinstellingen op de openbare website nextcloud.com niet te wijzigen.</p> <p>Breng beheerders op de hoogte van het bestaan van de zeven geïdentificeerde relevante logbestanden die door Nextcloud GmbH en haar subwerkers worden gegenereerd, en van de bewaartermijnen.</p> <p>Informeer beheerders over de inhoud van het activiteitenlogboek van het Zammad-supportticketsysteem en de bewaartermijn van 42 dagen.</p> | <p>De informatie over functionele cookies op het beheerders- en ondersteuningsportaal wordt in juli 2026 bijgewerkt</p> <p>Nextcloud heeft SURF aanvullende informatie verstrekt over de zeven logbestanden. Nextcloud zal deze informatie in juli 2026 op zijn openbare website publiceren (zoals goedgekeurd door SURF).</p> <p>Nextcloud zal deze informatie in juli 2026 op zijn openbare website publiceren (zoals beoordeeld door SURF).</p> | laag |

|    |                                                                                                     |                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |          |
|----|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 7. | Verlies van controle en gebrek aan transparantie bij subverwerkers                                  | -                                                                                                                                                                                           | Er is overeenstemming bereikt over de procedure voor het omgaan met wijzigingen in de gewijzigde DPA, zowel met betrekking tot nieuwe subverwerkers als tot andere wijzigingen.                                                                                                                                                                                                                                                                                                                                                                                                         | opgelost |
| 8. | Onvermogen om betrokken rechten uit te voeren                                                       | -                                                                                                                                                                                           | <p>Toezegging gedaan om volledige toegang te verlenen bij een inzageverzoek. Dit omvat toegang tot alle verzamelde gebruiksonderzoeksgegevens, activiteitenlogboeken van het ondersteuningsticketsysteem, bevroren webservertoegangslogboeken (op voorwaarde dat Nextcloud de identiteit van de betrokkene op betrouwbare wijze kan verifiëren) en logboeken die worden bijgehouden door Postmark (of een toekomstige in de EU gevestigde e-maildienstverlener).</p> <p><i>OPMERKING: SURF heeft dit niet opnieuw getest met een nieuw DSAR.</i></p>                                    | laag     |
| 9. | Onvermogen om het recht van de betrokkene op verwijdering van Ondersteuningsgegevens uit te oefenen | Geef beheerders de instructie om in ondersteuningstickets alleen strikt noodzakelijke persoonsgegevens te delen. Gebruik tickets niet om juridische of financiële vorderingen in te dienen. | <p>Nextcloud zal over het algemeen voldoen aan verzoeken tot verwijdering van een of meer ondersteuningstickets en/of bijlagen, tenzij er een wettelijke reden is om een specifiek ticket te bewaren.</p> <p>Nextcloud heeft voor SURF-leden een maximale bewaartermijn van 15 maanden overeengekomen voor afgesloten supporttickets.</p> <p>In de overeengekomen nieuwe openbare documentatie over de logbestanden die Nextcloud GmbH verzamelt en de bewaartermijnen staat vermeld dat Nextcloud de supporttickets over een specifiek onderwerp bij wijze van uitzondering langer</p> | laag     |

|     |                                                                                                                       |                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |          |
|-----|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|     |                                                                                                                       |                                                                                                                                                                               | mag bewaren, om een specifieke juridische reden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |          |
|     |                                                                                                                       |                                                                                                                                                                               | Nextcloud heeft al een waarschuwing tegen het delen van persoonsgegevens in bijlagen op het beheerdersportaal geïmplementeerd en zal de waarschuwing uiterlijk in het derde kwartaal van 2026 ook op het supportportaal weergeven.                                                                                                                                                                                                                                                                                                                                         |          |
|     |                                                                                                                       | Geef beheerders de instructie om Nextcloud jaarlijks te verzoeken alle supporttickets te verwijderen na de zelf vastgestelde bewaartermijn van bijvoorbeeld 13 of 15 maanden. | Overeengekomen in de gewijzigde DPA om als geautoriseerde verwerkingsverantwoordelijke uitsluitend geaggregeerde en gepseudonimiseerde gegevens uit supporttickets te verwerken die boven het tenant-niveau liggen.                                                                                                                                                                                                                                                                                                                                                        |          |
| 10. | Bekendmaking van verlies van controle over (beperkte) persoonsgegevens aan overheidsinstanties binnen en buiten de EU |                                                                                                                                                                               | <p>In de gewijzigde DPA is overeengekomen om de voorgestelde maatregelen ter risicobeperking te nemen. Nextcloud zal verzoeken van autoriteiten buiten de EU afwijzen. Nextcloud zal trachten verzoeken van EU-autoriteiten door te sturen naar zijn klant, deze waar mogelijk en haalbaar juridisch aanvechten, maar indien nodig slechts de minimaal noodzakelijke gegevens verstrekken.</p> <p>In de gewijzigde DPA is toegezegd om ten minste eenmaal per jaar transparantiestatistieken te publiceren, inclusief cijfers over ontvangen en beantwoorde verzoeken.</p> | laag     |
| 11. | Verlies van controle over                                                                                             | Waarschuw beheerders om hun beheerdersaccountgegevens                                                                                                                         | Er is overeenstemming bereikt over twee lijsten met doeleinden in de gewijzigde DPA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | opgelost |

|     |                                                                                     |                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                             |          |
|-----|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
|     | verwerkingen van Nextcloud als onafhankelijke verwerkingsverantwoordelijke          | niet te gebruiken om verwerking door Nextcloud of derden als onafhankelijke verwerkingsverantwoordelijke mogelijk te maken, bijvoorbeeld door toestemming te geven voor analytische en trackingcookies. Raad beheerders aan een pseudoniem account te gebruiken bij het registreren voor een evenement of bij het registreren om een whitepaper te downloaden. | In de gewijzigde DPA is overeengekomen om de huidige standaardinstellingen voor privacy te handhaven. Analyse- en marketingcookies worden alleen op de openbare website geplaatst na vrijwillige toestemming van de gebruiker.                                              |          |
| 12. | Verlies van controle: gebruik van tracking-pixels in uitgaande e-mail van Nextcloud | .                                                                                                                                                                                                                                                                                                                                                              | Nextcloud heeft de tracking-pixel in zijn emails uitgeschakeld.                                                                                                                                                                                                             | opgelost |
| 13. | Verlies van controle over gegevens van beheerders-accounts in nieuwsbrieven         | Geef beheerders de instructie om zich af te melden voor commerciële nieuwsbrieven.                                                                                                                                                                                                                                                                             | In het Nextcloud-zelfbedieningsportaal (portal.nextcloud.com) kunnen klanten zich in het derde kwartaal van 2026 registreren als beheerder of commercieel contactpersoon en zelf beslissen of ze zich willen aan- of afmelden voor commerciële en technische nieuwsbrieven. | laag     |
| 14. | Verlies van controle door gebrek aan transparantie over het bestaan van meerdere    | Gebruik de lijst in deze overkoepelende DPIA om beheerders bewust te maken van alle beschikbare logbestanden.                                                                                                                                                                                                                                                  | Nextcloud zal in het derde kwartaal van 2026 in de <a href="#">bestaande logboekdocumentatie</a> een beter overzicht van de beschikbare logboeken voor beheerders bieden.                                                                                                   | laag     |

|     |                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                |      |
|-----|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
|     | logbestanden in de software                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                |      |
| 15. | Chilling effect: monitoringssysteem voor medewerkers en studenten | <p>Maak beheerders bewust van de potentieel gevoelige inhoud van de (oorspronkelijke) audit- en Talk-interactielogboeken.</p> <p>Pas het interne IT-beleid aan om vast te leggen wanneer en voor welke doeleinden deze logbestanden legitiem mogen worden gebruikt.</p> <p>Om te voorkomen dat de audit- en interactielogboeken worden gebruikt als monitoringssysteem voor medewerkers, moet de gemaskeerde versie van de audit- en Talk-interactielogboeken in de SIEM- en logboekbeheertools worden geïmporteerd zodra deze beschikbaar is, en moet een passende bewaartermijn voor de ruwe gegevens worden vastgesteld.</p> | <p>Nextcloud heeft toegezegd om tegen eind 2026 een tweede exportversie van de audit- en interactielogboeken te ontwikkelen. Persoonsgegevens zoals vergader- en bestandsnamen worden gemaskeerd met ***VERWIJDERDE GEVOELIGE WAARDE***.</p> <p>Nextcloud zal de beschikbare informatie over de gevoelige inhoud in het derde kwartaal van 2026 bijwerken.</p> | laag |