Driving innovation together

DPIA TOPdesk

SURF Vendor Compliance

Let op: dit is een informele vertaling van het originele Engelse document, bij tegenstrijdigheden is de Engelse versie van de DPIA leidend.

Auteur(s)): Arnold Roosendaal, Winfried Tilanus, Evan Blommaert
Versie: 1.0
Datum: 15 januari 2026

Samenvatting

Dit rapport is een gegevensbeschermingseffectbeoordeling (DPIA) over het gebruik van TOPdesk voor het onderwijs (hierna: TOPdesk DPIA). Deze DPIA is geschreven voor Nederlandse onderzoeks- en onderwijsinstellingen, soms afgekort tot 'instellingen'. De eerste versie van deze DPIA is gepubliceerd op 15 januari 2026.

Toepassingsgebied: TOPdesk SaaS
TOPdesk is een cloudgebaseerd platform dat is ontworpen voor servicemanagement en een breed scala aan modules biedt, zoals verandermanagement, incidentmanagement en activabeheer. TOPdesk wordt gebruikt door een breed scala aan organisaties, van bedrijven tot overheidsinstanties. In de praktijk wordt het systeem vaak gebruikt om bedrijfs(IT)-middelen te beheren, incidenten te melden en/of als kennisbank. Binnen het Nederlandse onderwijs wordt TOPdesk gebruikt door beroepsopleidingen, hogescholen en universiteiten.

Deze DPIA beoordeelt de risico's voor de rechten en vrijheden van werknemers, studenten en andere betrokkenen van instellingen die verband houden met het gebruik van TOPdesk voor een aantal vooraf gedefinieerde gebruiksscenario's:
- TOPdesk als ticketsysteem voor IT-diensten
- TOPdesk als systeem voor incidentbeheer (afhandeling van informatiebeveiligingsincidenten en inbreuken op persoonsgegevens)
- TOPdesk voor registratie van ongevallen/ongepast gedrag in het kader van sociale veiligheid
- TOPdesk binnen de HR-afdeling voor de afhandeling van vragen en kwesties over integrale veiligheid, klachten en vertrouwelijkheid
- TOPdesk voor de verwerking van gevoelige informatie van apparaat-, incident-, applicatie- en klachtenbeheer

Daarnaast zijn risico's in verband met applicatie- en auditlogging en het instellen van autorisatie- en toegangsrechten binnen TOPdesk door instellingen aandachtspunten van deze DPIA.

Aangezien dit een overkoepelende DPIA is, bevat deze geen beoordeling van de rechtmatigheid van specifieke verwerkingsactiviteiten, noch van risico's die specifiek zijn voor individuele instellingen. Er wordt een meer algemene beoordeling gemaakt op basis van het beoogde gebruik van TOPdesk door instellingen. Verder vallen optionele componenten (zoals een livechatfunctie en een feedbackoplossing) en systemen van externe leveranciers die via een API met TOPdesk worden verbonden, buiten het bereik van de DPIA. Instellingen die TOPdesk willen gebruiken, kunnen deze DPIA als uitgangspunt nemen, maar moeten deze aanvullen, uitbreiden en/of aanpassen op basis van de specifieke context waarin zij TOPdesk willen gebruiken.

Methodologie
Deze DPIA is gebaseerd op:
- Deskresearch en juridische beoordeling van de documentatie, kennisbank, relevante voorwaarden, contracten en overeenkomsten van TOPdesk
- Verschillende interviews met vertegenwoordigers van TOPdesk, medewerkers van een onderwijsinstelling die TOPdesk gebruikt en vertegenwoordigers van SURF
- Technisch onderzoek ter plaatse bij een onderwijsinstelling, met behulp van een gespecialiseerde monitoringtool (man-in-the-middle proxy)
- Verzoeken om inzage van betrokkenen, ingediend na het technische onderzoek

- Beoordelingen door TOPdesk en SURF

De rol van de vertegenwoordigers van TOPdesk verdient een speciale vermelding. TOPdesk is zeer transparant geweest en heeft tijdens het hele proces proactief verschillende problemen opgelost. Bij verschillende gelegenheden, bijvoorbeeld toen de betrokkenheid van subverwerkers nodig was om de verzoeken om toegang van betrokkenen te beantwoorden, hebben de vertegenwoordigers van TOPdesk uitzonderlijke inspanningen geleverd om informatie te verkrijgen en aanvullende afspraken te maken.

Resultaat: 9 hoge en 3 lage risico's
Deze DPIA heeft negen hoge risico's en drie lage risico's voor de rechten en vrijheden van betrokkenen geïdentificeerd. Deze risico's zijn deels te wijten aan de manier waarop instellingen TOPdesk (waarschijnlijk) zullen gebruiken, en deels aan het ontwerp van TOPdesk zelf. Drie van de hoge risico's houden verband met de mogelijkheid dat een instelling bijzondere categorieën persoonsgegevens verwerkt in TOPdesk; als een instelling dit niet doet, zijn deze drie risico's niet van toepassing. Daarnaast ontstaan er risico's door de optionele inschakeling van (sub)verwerkers door TOPdesk of een instelling.

Voor alle risico's, inclusief de drie lage risico's, zijn maatregelen voorgesteld. Zeven van deze maatregelen zijn van toepassing op instellingen en tien op TOPdesk. Door deze maatregelen te implementeren worden alle hoge risico's beperkt, waardoor alleen lage restrisico's overblijven.

> **Update 12/12/2025:** Tijdens de uitvoering van de DPIA heeft TOPdesk al verschillende maatregelen genomen om de geïdentificeerde risico's te beperken. Meer specifiek heeft TOPdesk al maatregelen genomen voor vier hoge risico's (#2, 3, 8, 9) en maatregelen geïmplementeerd voor alle lage risico's. Voor één hoog risico zijn alleen maatregelen van de instelling nodig. Op het moment van schrijven blijven er dus vier hoge risico's over. Voor al deze risico's is een tijdlijn voor de implementatie van de maatregelen vastgesteld.

Een overzicht van alle geïdentificeerde risico's en voorgestelde maatregelen is weergegeven in de onderstaande tabel. Voor zover TOPdesk al maatregelen heeft genomen of heeft aangegeven maatregelen te willen nemen, is dit weergegeven in de rechterkolom.

Tabel1 : Overzicht risico's, maatregelen en status

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Status van TOPdesk-maatregel
1.	Verlies van controle – gebrek aan beleid voor het reguleren van persoonsgegevens in de logbestanden van TOPdesk	Geen	Een logbeleid opstellen en implementeren waarin wordt beschreven welke persoonsgegevens op elk logniveau worden geregistreerd.	TOPdesk heeft een logbeleid opgesteld dat door alle afdelingen moet worden geïmplementeerd. De deadline hiervoor is het

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Status van TOPdesk-maatregel
				vierde kwartaal van 2026.
2.	Verlies van controle bij het sluiten van contracten op basis van de TOPdesk template verwerkers-overeenkomst – gebruik van optionele subverwerkers van TOPdesk	Zorg ervoor dat de verwerkersovereen komst tussen de instelling en TOPdesk een weerspiegeling is van de subverwerkers die daadwerkelijk worden ingeschakeld	Definieer optionele subverwerkers in de tabel op de SaaS-website.	Sinds 06-10-2025 vermeldt de SaaS-informatiepagin a van TOPdesk welke subverwerkers optioneel zijn en informeert het klanten dat ze de toepasselijke subverwerkers kunnen vinden in hun hoofdovereenko mst. Door deze maatregel is het risico nu laag.
3.	Verlies van controle – Actief abonnement vereist voor updates over de subverwerkers van TOPdesk	Geen	Alle verwerkingsverantwoo rdelijken actief informeren over wijzigingen in subverwerkers en voor elke wijziging toestemming vragen.	Op 09-10-2025 heeft TOPdesk zijn beleid aangepast. Nu ontvangen alle geregistreerde SaaS-hoofdcontactper sonen standaard een melding van een nieuwe subverwerker. Door deze geïmplementeer de maatregel is het risico nu laag.

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Status van TOPdesk-maatregel
4.	Verlies van controle – Overdracht van persoonsgegevens via Cloudflare niet weergegeven in verwerkersovereenkomst	Zorg ervoor dat de doorgifte van persoonsgegevens via Cloudflare correct wordt weergegeven in de verwerkersovereenkomst en voldoet aan hoofdstuk V van de AVG.	Wijzig de TOPdesk-sjabloon verwerkersovereenkomst om de doorgifte van persoonsgegevens naar Cloudflare weer te geven	Dit risico is laag, dus er zijn geen maatregelen verplicht, maar TOPdesk zal deze maatregel in het eerste kwartaal van 2026 implementeren.
5.	Verlies van controle – inzageverzoeken van buiten de EER bij Cloudflare			Dit risico is laag, dus er zijn geen maatregelen verplicht. TOPdesk blijft echter mogelijke openbaarmakingen door Cloudflare monitoren.
6.	Verlies van controle – doorgifte van persoonsgegevens via Microsoft			Dit risico is laag, dus er zijn geen maatregelen verplicht. TOPdesk blijft echter mogelijke openbaarmakingen door Microsoft monitoren.
7.	Verlies van controle – automatische anonimisering mislukt voor derde betrokkenen	Implementeer een van de volgende maatregelen of een combinatie daarvan: • Een beleid om geen persoonsgegevens over derden op te nemen in de vrije	Geen	Niet van toepassing

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Status van TOPdesk-maatregel
		tekstvelden van een kaart • Een beleid om de vrije tekstvelden van een kaart handmatig te anonimiseren • Een beleid om kaarten niet te anonimiseren, maar te verwijderen na hun bewaartermijn		
8.	Onvermogen om de rechten van de betrokkene uit te oefenen – Niet-tijdige hulp van Cloudflare en Microsoft	Geen	Een procedure implementeren om persoonsgegevens uit de logbestanden van Cloudflare te verstrekken.	Op 17-09-2025 heeft TOPdesk een procedure geïmplementeerd voor het verstrekken van persoonsgegevens uit de logbestanden van Cloudflare. Door deze maatregel is het risico nu laag.
9.	Onvermogen om rechten van betrokkenen uit te oefenen – Gegevens onzichtbaar voor beller	Implementeer een procedure om onzichtbare antwoorden op te nemen in de antwoorden op verzoeken van betrokkenen.	Geen	Op 18-11-2025 heeft TOPdesk de noodzaak om deze procedure te implementeren toegevoegd aan de best

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Status van TOPdesk-maatregel
				practices in de kennisbank.
Risico's en maatregelen voor instellingen die bijzondere categorieën persoonsgegevens verwerken met TOPdesk				
#	**Risico**	**Maatregelen Instelling**	**Maatregelen TOPdesk**	**Status van TOPdesk-maatregel**
10.	Verlies van vertrouwelijkheid en onrechtmatige verdere verwerking – Gebruik van bijzondere categorieën persoonsgegevens in test- of stagingomgeving	Maak gebruik van de optie om databasequery's uit te voeren om persoonsgegevens uit de productieomgeving te vervangen door synthetische gegevens voordat de gegevens naar een test- of stagingomgeving worden gekopieerd	Bied de mogelijkheid om automatisch het tabblad 'Privé' en 'Contract' van de kaarten te verwijderen bij het overzetten van productiegegevens naar een test- of stagingomgeving.	TOPdesk heeft aangegeven dat zij bezig zijn met de implementatie van deze maatregel. De deadline is Q2 2026. Daarnaast heeft TOPdesk op 18-11-2025 de noodzaak om deze procedure te implementeren toegevoegd aan de best practices in de kennisbank.
11.	Verlies van controle – Verwerking van bijzondere categorieën persoonsgegevens in TOPdesk	Voer de juiste compliance-werkzaamheden uit voordat u bijzondere categorieën persoonsgegevens in TOPdesk verwerkt, om ervoor te zorgen dat de instelling een beroep kan doen op een van de uitzonderingen in artikel 9, lid 2, van de AVG.	Maak of update een kennisitem voor instellingen met informatie en best practices over de verwerking van bijzondere categorieën gegevens in TOPdesk.	TOPdesk heeft aangegeven dat deze maatregel naar verwachting eind Q4 2025 zal zijn geïmplementeerd.

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Status van TOPdesk-maatregel
		Zorg ervoor dat bij de verwerking van bijzondere categorieën persoonsgegevens in TOPdesk dit correct wordt weergegeven in de verwerkersovereen komst met TOPdesk.		
		Configureer geen (medische) aandoeningen in Attenties, maar relevante acties die een operator moet ondernemen.		
		Maak bij het registreren van bijzondere categorieën persoonsgegevens van een betrokkene gebruik van het tabblad 'Privé' op de persoonskaart in de module Ondersteunende bestanden (zie §**Fout! Verwijzingsbron niet gevonden.**).		
12.	Verlies van controle – onvoldoende auditlogging van bijzondere categorieën gegevens	Bij gebrek aan implementatie door TOPdesk van aanvullende logging bij toegang tot en wijziging van het privétabblad: Implementeer auditlogging bij toegang tot kaarten van processen die waarschijnlijk	Implementeer aanvullende auditlogging: log wie welke kaart wanneer heeft geopend en voeg deze optie toe aan aangepaste logacties.	TOPdesk zal standaard extra logging implementeren voor toegang tot en wijziging van het privétabblad op de persoonskaart. Dit staat gepland voor het

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Status van TOPdesk-maatregel
		speciale categorieën gegevens bevatten.		eerste kwartaal van 2026.
		Nadat TOPdesk extra logging heeft geïmplementeerd voor toegang tot en wijziging van het privétabblad: maak gebruik van het privétabblad op persoonskaarten om bijzondere categorieën gegevens te verwerken.		

Deel C: Beschrijving van de risico's

Dit deel betreft de beschrijving en beoordeling van de risico's voor betrokkenen. In dit deel wordt gekeken naar zowel de risico's die verband houden met het sleutelbeheer als de risico's die verband houden met de verwerking van persoonsgegevens door de systeembeheerders. De risico's worden vervolgens ingedeeld naar de waarschijnlijkheid dat ze zich voordoen en de gevolgen voor de rechten en vrijheden van de betrokkenen wanneer ze zich voordoen.

1. Risico's

Dit deel betreft de beschrijving en beoordeling van de risico's voor betrokkenen. Dit zijn de risico's die tijdens het testen en analyseren en vóór het nemen van mitigerende maatregelen zijn geconstateerd. De risico's worden vervolgens ingedeeld naar de waarschijnlijkheid dat ze zich voordoen en de gevolgen voor de rechten en vrijheden van de betrokkenen wanneer ze zich voordoen. Het model van deze DPIA, gebaseerd op "het Rijksmodel", maakt gebruik van de risicocategorieën en het risicomodel van de Britse gegevensbeschermingsautoriteit, ICO. ICO somt de volgende hoofdcategorieën van risico's op:

- Verlies van controle over persoonsgegevens
- Verlies van vertrouwelijkheid
- Onmogelijkheid voor de betrokkenen om hun rechten uit te oefenen
- Heridentificatie van gepseudonimiseerde persoonsgegevens
- Onrechtmatige verdere verwerking

Deze hoofdcategorieën bieden houvast bij het bepalen van specifieke risico's. Door de risico's weer te geven op basis van hun potentiële impact op de rechten en vrijheden van betrokkenen, ontstaat een beeld van de hoge en lage risico's. Dit wordt weergegeven in de risicograaf die is ontwikkeld door de Britse toezichthouder ICO, als volgt:

Tabel2 : ICO-risicomodel

Ernst van de impact	Ernstige schade	Laag risico	Hoog risico	Hoog risico
	Enige impact	Laag risico	Gemiddeld risico	Hoog risico
	Minimale impact	Laag risico	Laag risico	Laag risico
		Zeer klein	Redelijke mogelijkheid	Waarschijnlijker wel dan niet
		Kans op schade		

Deze DPIA gebruikt de volgende betekenissen van de "kans op schade" en de "ernst van de gevolgen" om de risico's te beoordelen:

Tabel3 : Definities van waarschijnlijkheid:

Waarschijnlijkheid	Betekenis
Zeer klein	Het is onwaarschijnlijk dat dit risico zich zal voordoen
Redelijke kans	Het is denkbaar dat dit risico zich voordoet.
Waarschijnlijker wel dan niet	Het is waarschijnlijk of zeker dat het risico zich zal voordoen

Tabel4 : Definities van impact

Impact	Betekenis
Minimale impact	De gevolgen voor de betrokkene hebben weinig of geen invloed op de rechten en vrijheden van de betrokkene wanneer het risico zich voordoet.

Enige impact	De gevolgen voor de betrokkene hebben een beperkte impact op de rechten en vrijheden van de betrokkene wanneer het risico zich voordoet.
Ernstige schade (ernstige impact)	De gevolgen voor de betrokkene hebben een aanzienlijke impact op de rechten en vrijheden van de betrokkene wanneer het risico zich voordoet

1.1 Identificatie van gegevensbeschermingsrisico's

Bij het uitvoeren van deze DPIA zijn de volgende risico's geïdentificeerd:

Tabel5 : risico-overzicht

#	Risico	Type risico	Waarschijnlijkheid	Impact
1.	Gebrek aan beleid voor het reguleren van persoonsgegevens in de logbestanden van TOPdesk	Verlies van controle	Waarschijnlijker wel dan niet	Ernstige impact
2.	Gebruik van optionele subverwerkers	Verlies van controle – contract op basis van TOPdesk-sjabloon verwerkersovereenkomst	Redelijke mogelijkheid	Ernstige gevolgen
3.	Actief abonnement vereist voor updates over de subverwerkers van TOPdesk	Verlies van controle	Redelijke mogelijkheid	Ernstige gevolgen
4.	Overdracht van persoonsgegevens via Cloudflare	Verlies van controle	Waarschijnlijker wel dan niet	Minimale impact
5.	Toegangsverzoeken van buiten de EER bij Cloudflare	Verlies van controle	Kleine kans	Ernstige impact
6.	Overdracht van persoonsgegevens via Microsoft	Verlies van controle	Kleine kans	Ernstige gevolgen
7.	Automatische anonimisering mislukt voor derde betrokkenen	Verlies van controle	Redelijke mogelijkheid	Ernstige gevolgen
8.	Te late hulp van Cloudflare en Microsoft	Onvermogen om de rechten van de betrokkene uit te oefenen	Waarschijnlijker wel dan niet	Ernstige gevolgen
9.	Gegevens onzichtbaar voor beller	Onvermogen om rechten van betrokkenen uit te oefenen	Redelijke mogelijkheid	Ernstige gevolgen

#	Risico	Type risico	Waarschijnlijkheid	Impact
Risico's die van toepassing zijn op instellingen die bijzondere categorieën persoonsgegevens verwerken met TOPdesk				
#	**Risico**	**Type risico**	**Waarschijnlijkheid**	**Impact**
10.	Gebruik van speciale categorieën persoonsgegevens in test- of stagingomgevingen	Verlies van vertrouwelijkheid en onrechtmatige verdere verwerking	Redelijke mogelijkheid	Ernstige gevolgen
11.	Verwerking van bijzondere categorieën persoonsgegevens in TOPdesk	Verlies van controle	Redelijke mogelijkheid	Ernstige gevolgen
12.	Onvoldoende auditlogging van bijzondere categorieën gegevens	Verlies van controle	Redelijke mogelijkheid	Ernstige gevolgen

Hieronder volgt een toelichting op de risico's. Deze zijn onderverdeeld in 'Algemene risico's', die van toepassing kunnen zijn op alle instellingen die TOPdesk gebruiken voor de in deze DPIA beoordeelde gebruikssituaties, en 'Risico's in verband met de verwerking van bijzondere categorieën persoonsgegevens met TOPdesk', aangezien niet alle instellingen bij het gebruik van TOPdesk bijzondere categorieën persoonsgegevens verwerken.

1.2 Algemene risico's

1.2.1 Verlies van controle – gebrek aan beleid voor het reguleren van persoonsgegevens in de logbestanden van TOPdesk (risico # 1)

TOPdesk heeft aangegeven dat zij een algemeen beleid hebben om het opslaan van persoonsgegevens in logbestanden te beperken tot wat noodzakelijk is. TOPdesk heeft echter geen specifiek beleid over welke soorten persoonsgegevens precies worden gelogd voor elk verschillend logniveau. Als gevolg hiervan worden persoonsgegevens gelogd op logniveaus waar dat type persoonsgegevens niet verwacht wordt en ook niet hoeft te worden gelogd.

De kans dat dit gebeurt is groter dan niet, aangezien dit de feitelijke situatie is. De schade voor de rechten en vrijheden van de betrokkenen is ernstig, omdat de instelling geen controle heeft over welke gegevens op welk logniveau worden geregistreerd, waardoor pogingen om het registreren van persoonsgegevens en het opslaan van persoonsgegevens in logbestanden tot een minimum te beperken, kunnen mislukken. Daarom is dit risico groot.

1.2.2 Verlies van controle bij het aangaan van contracten op basis van het TOPdesk-sjabloon verwerkersovereenkomst – gebruik van optionele subverwerkers van TOPdesk (risico # 2)

Instellingen kunnen ervoor kiezen om gebruik te maken van de optionele extra functies in TOPdesk die worden gefaciliteerd door Hello Ebbot AB, voor Live Chat- en AI Chatbot-functionaliteiten, en Insocial, dat feedbackoplossingen biedt. Als een instelling hiervoor

kiest, moet dit worden vastgelegd in de verwerkersovereenkomst tussen de instelling en TOPdesk. In het SURF-sjabloon voor de verwerkersovereenkomst worden de toepasselijke subverwerkers specifiek vermeld. De TOPdesk-sjabloon verwerkersovereenkomst verwijst echter naar een TOPdesk-website voor een overzicht van de toepasselijke subverwerkers.[1] Op deze website staan alle feitelijke en potentiële subverwerkers van TOPdesk vermeld. Gezien deze opzet in de TOPdesk-model-verwerkersovereenkomst is het niet (onmiddellijk) duidelijk welke subverwerkers betrokken zijn bij de daadwerkelijke verwerking van persoonsgegevens van betrokkenen van instellingen. Zonder duidelijkheid over welke subverwerkers feitelijk bij de verwerking betrokken zijn, is er onvoldoende controle over die verwerking.

De kans dat dit risico schade toebrengt aan de rechten en vrijheden van de betrokkene is redelijk; de lijst is beschikbaar op de website, dus instellingen hebben wel degelijk middelen om controle te houden, maar daarvoor zouden instellingen een beleid/procedure moeten hebben om die website actief te monitoren. Verlies van controle doet zich voor wanneer de verwerkingsverantwoordelijken de betrokkenen niet naar behoren informeren over de verwerking van hun persoonsgegevens door subverwerkers. Zonder de juiste informatie zijn zij niet in staat om effectieve controle uit te oefenen over hun persoonsgegevens, wat tot ernstige schade kan leiden. Gezien de redelijke waarschijnlijkheid, in combinatie met de ernstige gevolgen, is dit risico hoog.

1.2.3 Verlies van controle – actieve aanmelding vereist voor updates over subverwerkers van TOPdesk (risico # 3)

Instellingen moeten zich actief aanmelden via een TOPdesk-website om updates over wijzigingen in subverwerkers te ontvangen. Instellingen die zich niet actief aanmelden (en zich niet realiseren dat ze dat moeten doen), worden niet op de hoogte gebracht van dergelijke wijzigingen en kunnen hun betrokkenen dus niet informeren, die op hun beurt het risico lopen de controle te verliezen over hun persoonsgegevens die door subverwerkers worden verwerkt. Bovendien is het onduidelijk hoe instellingen die zich niet actief aanmelden voor updates toestemming moeten geven voor wijzigingen in subverwerkers. Als TOPdesk in dergelijke gevallen geen toestemming vraagt aan instellingen via , is dit een schending van zowel het SURF-model verwerkersovereenkomst als het TOPdesk-model verwerkersovereenkomst.

De kans dat dit gebeurt is redelijk groot, aangezien instellingen zelf moeten opmerken dat ze zich actief moeten aanmelden voor updates. Zonder de juiste informatie kunnen betrokkenen geen effectieve controle uitoefenen over hun persoonsgegevens, wat tot ernstige schade kan leiden. Het algehele risico is hoog.

1.2.4 Verlies van controle – doorgifte van persoonsgegevens via Cloudflare niet weergegeven in verwerkersovereenkomst (risico # 4)

Volgens de TOPdesk-model-verwerkersovereenkomst en de SURF-model-verwerkersovereenkomst die in deze DPIA zijn beoordeeld, vindt er geen doorgifte van persoonsgegevens plaats door het gebruik van TOPdesk door instellingen. Uit technisch onderzoek blijkt echter dat IP-adressen van betrokkenen worden overgedragen aan Cloudflare in de VS in het kader van DDoS-bescherming. Bovendien wordt deze doorgifte vermeld in de verwerkersovereenkomst tussen TOPdesk en Cloudflare en heeft TOPdesk

[1] TOPdesk-sjabloon Verwerkingsovereenkomst, v. 2025, p. 10.

aangegeven dat deze doorgifte technisch niet kan worden voorkomen. De doorgifte vormt een schending van de verwerkersovereenkomst tussen TOPdesk en een instelling en leidt tot een verlies van controle over persoonsgegevens voor betrokkenen.

De kans dat dit gebeurt is groter dan niet, aangezien uit technisch onderzoek blijkt dat de doorgifte feitelijk plaatsvindt. De impact voor betrokkenen is echter minimaal, omdat de doorgifte alleen IP-adressen zonder enige context betreft. Deze kunnen bijvoorbeeld niet worden gebruikt om betrokkenen te discrimineren of uit te sluiten. Aangezien deze doorgifte echter niet is vastgelegd in de verwerkersovereenkomst, is er sprake van een schending van de AVG en de verwerkersovereenkomst. Dit kan op zijn beurt leiden tot verlies van controle over de overgedragen persoonsgegevens. Aangezien zowel de AVG als de verwerkersovereenkomst bedoeld zijn om de rechten en vrijheden van betrokkenen te waarborgen, leidt het ontbreken van dergelijke waarborgen tot risico's voor de rechten en vrijheden van betrokkenen. Het bijbehorende risico is laag.

1.2.5 Verlies van controle – verzoeken om toegang tot ex-EER- en bij Cloudflare (risico # 5)

Cloudflare verwerkt de lijst met IP-adressen die Cloudflare wereldwijd blokkeert. Deze lijst met IP-adressen kan de IP-adressen van eindgebruikers van TOPdesk bevatten, bijvoorbeeld wanneer zij zijn geïnfecteerd met malware. Door de wereldwijde verwerking valt deze lijst onder de reikwijdte van niet-EU-wetgeving en is deze daarom onderworpen aan niet-EU-procedures voor toegang tot de gegevens door wetshandhavingsinstanties. Cloudflare houdt toezicht op dergelijke toegang in hun transparantierapport. Daarnaast heeft Cloudflare canary-bepalingen in hun transparantierapport, die TOPdesk controleert.

Vanwege de zeldzaamheid van dit soort juridische verzoeken en omdat slechts een zeer klein deel van de eindgebruikers van TOPdesk in deze lijst is opgenomen, is de kans dat dit gebeurt zeer klein. Wanneer dit echter gebeurt, leidt dit tot een verlies van controle voor betrokkenen, wat kan leiden tot ernstige schade aan hun rechten en vrijheden, zoals vervolging in een land buiten de EER. Als zodanig is dit risico laag.

1.2.6 Verlies van controle – doorgifte van persoonsgegevens via Microsoft (risico # 6)

TOPdesk implementeert versleuteling voor de gegevens die bij Microsoft zijn opgeslagen, in combinatie met Microsoft 'Customer-managed keys', ondersteund door een hardwarebeveiligingsmodule. Deze opzet biedt TOPdesk echter geen volledige controle over de sleutels en gegevens. Hoewel er geen aanwijzingen zijn dat het gebruik van TOPdesk door instellingen leidt tot de doorgifte van persoonsgegevens via Microsoft, heeft TOPdesk verklaard dat deze doorgifte technisch niet kan worden uitgesloten.

Bovendien sluit de verwerkersovereenkomst tussen TOPdesk en Microsoft dergelijke doorgifteen niet uit en ontbreekt een canary-clausule voor wanneer een entiteit buiten de EER gegevens opvraagt bij Microsoft, in combinatie met een spreekverbod. Daarom bestaat het risico dat een dergelijke doorgifte plaatsvindt, wat zou leiden tot een verlies van controle over persoonsgegevens voor betrokkenen. Omdat niet-regelmatige doorgifteen zeldzaam zijn, is de kans dat dit gebeurt zeer klein. Wanneer dit gebeurt, leidt dit tot een verlies van controle voor betrokkenen, wat kan leiden tot ernstige schade aan de rechten en vrijheden van de betrokkene. Daarom is dit risico laag.

1.2.7 Verlies van controle – anonimisering maakt gegevens over betrokkenen die in kaarten worden vermeld niet anoniem (risico # 7)

Het geautomatiseerde proces voor het anonimiseren van gegevens herkent alleen persoonsgegevens van de gekoppelde personenkaarten. Als de kaart die geanonimiseerd moet worden gegevens bevat over een betrokkene die niet op een gekoppelde personenkaart staat, worden deze gegevens niet geanonimiseerd. Om te voorkomen dat deze persoonsgegevens langer worden bewaard dan het bewaarbeleid voorschrijft, moeten deze kaarten handmatig worden gewist of volledig worden verwijderd. Als de kaarten niet worden geanonimiseerd of verwijderd, leidt dit tot opslag van persoonsgegevens buiten het bewaarbeleid van de instelling.

Het is moeilijk om dit risico nauwkeurig in te schatten, omdat het verband houdt met de mogelijkheid dat een instelling onvoldoende maatregelen heeft genomen, waardoor het onduidelijk is of er aanvullende stappen nodig zijn om persoonsgegevens volledig te anonimiseren. Aangezien dit op basis van deze DPIA niet nauwkeurig kan worden beoordeeld, wordt de mogelijkheid als redelijk beschouwd. De potentiële impact van dit risico is gemakkelijker in te schatten. Als het risico zich voordoet, worden persoonsgegevens langer dan nodig opgeslagen, wat in strijd is met het beginsel van opslagbeperking. Het schenden van een basisbeginsel van de AVG heeft ernstige gevolgen voor de rechten en vrijheden van betrokkenen. Daarom is dit risico hoog.

1.2.8 Onvermogen om de rechten van betrokkenen uit te oefenen – niet-tijdige hulp van Cloudflare en Microsoft op basis van de verwerkersovereenkomst (risico # 8)

Als onderdeel van deze DPIA werd een verzoek om toegang van de betrokkene ingediend bij TOPdesk door de instelling waar het technische onderzoek werd uitgevoerd. Het verzoek om toegang bevatte ook vragen over de verwerking door Cloudflare en Microsoft. Daarom heeft TOPdesk Cloudflare en Microsoft om hulp gevraagd om aan het verzoek te kunnen voldoen. Cloudflare en Microsoft hebben echter geen tijdige reactie gegeven. Hierdoor moest TOPdesk de termijn om aan het verzoek te voldoen met twee maanden verlengen, overeenkomstig artikel 12, lid 3, van de AVG.

Uiteindelijk heeft Cloudflare TOPdesk een procedure verstrekt om de logbestanden zelf te downloaden en te analyseren. Tegen de tijd dat deze procedure was ingevoerd, was een deel van de logbestanden echter al verwijderd vanwege een bewaartermijn van 30 dagen. Nu deze procedure is ingevoerd, kan TOPdesk binnen 30 dagen volledig voldoen aan deze verzoeken met betrekking tot Cloudflare-logbestanden.

Ruim na de verlengde termijn van twee maanden kon TOPdesk bij Microsoft bevestigen dat de opgevraagde logbestanden geen IP-adressen bevatten.

De kans dat dit risico zich voordoet, is groter dan niet: zoals tijdens de DPIA is gebleken, kon TOPdesk de termijn van twee maanden niet halen vanwege te late hulp van zijn subverwerkers. Het niet halen van de deadline leidt tot ernstige schade aan de rechten van de betrokkene. Daarom is dit risico groot.

1.2.9 Onvermogen om de rechten van de betrokkene uit te oefenen – gegevens 'onzichtbaar voor een beller' (risico # 9)

Wanneer operators een oproep beantwoorden, kunnen ze ervoor kiezen om hun antwoord 'onzichtbaar voor de beller' te maken, zodat ze intern over de oproep kunnen communiceren. Deze notities zijn gekoppeld aan een beller en zijn daarom persoonsgegevens en onderworpen aan de rechten van de betrokkene. De instelling moet deze gegevens echter actief aan de betrokkene verstrekken, omdat ze niet toegankelijk zijn via het selfserviceportaal dat voor de betrokkene beschikbaar is. Wanneer de instelling niet over een goede procedure beschikt om ook deze gegevens te verstrekken, kan de betrokkene zijn rechten niet uitoefenen.

Wanneer een instelling een verzoek om toegang van een betrokkene ontvangt, is het standaardantwoord voor TOPdesk om te verwijzen naar het selfserviceportaal, omdat daar normaal gesproken alle gegevens beschikbaar zijn. Wanneer de kaart echter antwoorden bevat die 'onzichtbaar zijn voor de beller', moet de privacyfunctionaris, supportmedewerker of systeembeheerder die de vraag beantwoordt, de onzichtbare antwoorden handmatig verstrekken. Zij moeten zich hiervan bewust zijn en moeten hiervoor een procedure hebben. Omdat dit niet vanzelfsprekend is bij de implementatie van TOPdesk, bestaat er een redelijke kans dat deze gegevens niet worden verstrekt. De schade voor de betrokkene wanneer de gegevens niet worden verstrekt, is ernstig, omdat de betrokkene dan zijn (fundamentele) rechten uit hoofde van de AVG niet naar behoren kan uitoefenen. Daarom is dit risico groot.

1.3 Risico's voor instellingen die bijzondere categorieën persoonsgegevens verwerken met TOPdesk

Let op: de hieronder beschreven risico's zijn alleen van toepassing voor zover een instelling TOPdesk gebruikt om bijzondere categorieën persoonsgegevens te verwerken.

1.3.1 Verlies van vertrouwelijkheid en onrechtmatige verdere verwerking – gebruik van bijzondere categorieën persoonsgegevens in een test- of stagingomgeving (risico # 10)

Als instellingen een kopie van hun productieomgeving (die bijzondere categorieën persoonsgegevens kan bevatten) gebruiken om een test- of stagingomgeving op te zetten, is de kans op inbreuken op persoonsgegevens groter omdat instellingen over het algemeen minder streng zijn bij de toepassing van hun informatiebeveiligingsbeleid op test- of stagingomgevingen. In deze omgevingen worden bijvoorbeeld gemakkelijker machtigingen verleend, wat betekent dat personen die normaal gesproken geen toegang hebben tot (bijzondere categorieën) persoonsgegevens in de productieomgeving, via de test- of stagingomgeving toegang kunnen krijgen tot deze gegevens. Bovendien creëert het maken van een volledige kopie van een productieomgeving in een test- of stagingomgeving een tweede aanvalsoppervlak, waardoor de kans op een inbreuk op persoonsgegevens toeneemt. De kans is groot dat instellingen die een test- of stagingomgeving willen opzetten, een kopie van hun (volledige) productieomgeving maken, omdat:

- de standaard set synthetische gegevens die op verzoek bij TOPdesk beschikbaar is, mogelijk niet voldoende is. De synthetische gegevens zijn namelijk niet afgestemd op de aangepaste processen die de organisatie heeft gedefinieerd en zijn daarom mogelijk beperkt bruikbaar; en

- het handmatig aanmaken van databasequery's om synthetische gegevens te genereren voor instellingen een relatief arbeidsintensief proces is.

Het kopiëren van (bijzondere categorieën) persoonsgegevens van een productieomgeving naar een test- of stagingomgeving kwalificeert als een verdere verwerkingsactiviteit (bijv. artikel 6, lid 4, AVG) en moet daarom verenigbaar zijn met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld, rekening houdend met verschillende factoren. Als instellingen de betrokkenen echter niet naar behoren informeren over deze verdere verwerking, of als bijvoorbeeld het informatiebeveiligingsbeleid minder strikt wordt toegepast op de persoonsgegevens in de test- of stagingomgeving, is deze verdere verwerkingsactiviteit hoogstwaarschijnlijk onwettig. Dit geldt met name wanneer de persoonsgegevens speciale categorieën persoonsgegevens omvatten, omdat de drempel voor verenigbaarheid in dergelijke gevallen aanzienlijk hoger is en aanvullende maatregelen *moeten* worden genomen.

TOPdesk reageert op dit risico als volgt:

> "Acceptatieomgevingen worden doorgaans alleen gebruikt door applicatiebeheerders die al veel rechten hebben. Wanneer andere gebruikers toegang krijgen tot de acceptatieomgeving, blijven databasefilters van kracht en beperken deze de toegang tot gevoelige gegevens. Wanneer TOPdesk volgens best practices wordt gebruikt, is er een aparte rechtengroep voor toegang tot gevoelige persoonsgegevens, die u niet hoeft toe te kennen aan collega's om een effectieve test uit te voeren.
> Ten slotte blijven de gegevens in alle gevallen binnen dezelfde organisatie. Dit zijn collega's die doorgaans gebonden zijn aan een geheimhoudingsverklaring en er ook belang bij hebben om interne gegevens intern te houden."

Uit observaties tijdens het testen bleek echter dat applicatiebeheerders zich in de testomgeving minder terughoudend opstelden dan ze in de productieomgeving zouden hebben gedaan. Daarom kunnen speciale categorieën gegevens die voor hen in de productieomgeving niet toegankelijk zouden zijn geweest, wel toegankelijk zijn in de testomgeving.

Omdat tijdens het technisch onderzoek werd ontdekt dat de instelling waar het onderzoek werd uitgevoerd, productiegegevens met speciale categorieën gegevens verwerkte in een testomgeving, wordt aangenomen dat er een redelijke kans bestaat dat andere instellingen dit ook doen. De mate van schade wanneer speciale categorieën gegevens worden verwerkt in de testomgeving is ernstig, omdat deze gegevens onrechtmatig worden verwerkt. Daarom is dit risico hoog.

1.3.2 Verlies van controle – Verwerking van bijzondere categorieën persoonsgegevens in TOPdesk (risico # 11)

Instellingen kunnen alle soorten persoonsgegevens in TOPdesk verwerken, inclusief bijzondere categorieën van persoonsgegevens. Gezien de beoogde gebruikssituaties die in deze verwerkersovereenkomst worden beoordeeld – met name met betrekking tot het gebruik van TOPdesk door instellingen voor incidentregistratie of voor de registratie van ongevallen/ongepast gedrag in het kader van de sociale veiligheid – bestaat de kans dat bijzondere categorieën van persoonsgegevens worden verwerkt. Ook kan de instelling 'aandachtspunten' configureren die verband houden met personen, zoals 'is slechtziend'.

Als verwerkingsverantwoordelijke moet een instelling zelf bepalen of zij zich kan beroepen op een van de uitzonderingen in artikel 9, lid 2, AVG om de verwerking te legitimeren. Als een instelling voornemens is bijzondere categorieën gegevens in TOPdesk te verwerken, moet dit bovendien adequaat worden weergegeven in de verwerkersovereenkomst tussen de instelling en TOPdesk om de betrokkenen voldoende controle te bieden. Niet alle instellingen gebruiken TOPdesk voor processen waarbij bijzondere categorieën gegevens worden verwerkt, maar sommige wel. Wanneer zij dat doen – en geen van de uitzonderingen in artikel 9, lid 2, AVG van toepassing is – doet dit risico zich voor.

Om de waarschijnlijkheid dat dit risico zich voordoet te beoordelen, moet worden bepaald hoe groot de kans is dat een instelling nalaat de vereiste nalevingswerkzaamheden uit te voeren. Op basis van deze DPIA kan hierover geen onderbouwde uitspraak worden gedaan, hoewel tijdens het technische onderzoek anekdotisch bewijs is gevonden van onvoldoende governance van bijzondere categorieën gegevens. Voor deze risicobeoordeling wordt daarom aangenomen dat er een redelijke kans bestaat dat instellingen nalaten alle vereiste nalevingswerkzaamheden uit te voeren. Wanneer dit gebeurt, is de verwerking waarschijnlijk onrechtmatig en in strijd met de AVG, wat leidt tot ernstige schade voor de rechten en vrijheden van de betrokkene. Dit risico is dan ook groot.

1.3.3 Verlies van controle – onvoldoende auditlogging van bijzondere categorieën gegevens (risico # 12)

Naast de 'standaard' geconfigureerde logboeken kunnen instellingen ook een audittrail (met logboekvermeldingen) definiëren binnen hun eigen TOPdesk-omgeving. Voor processen die waarschijnlijk bijzondere categorieën van persoonsgegevens bevatten, is een uitgebreide audittrail nodig, waarin wordt vermeld wie toegang heeft gehad tot de gegevens. Dit moet door instellingen worden geïmplementeerd als aangepaste gebeurtenissen die in de audittrail moeten worden opgenomen. Als dit niet gebeurt, leidt dit tot verlies van controle over wie toegang heeft gehad tot bijzondere categorieën van gegevens. Dit risico geldt alleen voor zover bijzondere categorieën persoonsgegevens door een instelling in TOPdesk worden verwerkt, aangezien de aard van de andere gegevens in TOPdesk niet zo gevoelig is: deze bevatten hoogstwaarschijnlijk geen exacte locatiegegevens, beoordelingen van studie- of werkgerelateerde prestaties of andere gevoelige informatie. Daarom levert het ontbreken van auditlogging bij de verwerking van reguliere persoonsgegevens in TOPdesk geen significante risico's op, en zou aanvullende logging in feite onevenredig zijn.

Deze logboeken moeten handmatig worden geconfigureerd, afhankelijk van welke velden gegevens bevatten die extra logging vereisen. Omdat dit niet standaard is bij het configureren van de workflows in TOPdesk, is de kans redelijk groot dat de instelling dit niet implementeert. De schade voor de betrokkene wanneer dit deel van het controlespoor ontbreekt, is ernstig, omdat speciale categorieën gegevens worden verwerkt zonder voldoende toezicht op wie er toegang toe heeft gehad, wat kan leiden tot onrechtmatige verwerking. Daarom is dit risico hoog.

1.4 Risicomatrix

Door de risico's weer te geven op basis van hun potentiële impact op de rechten en vrijheden van betrokkenen, ontstaat een beeld van de hoge en lage risico's die gepaard gaan met de verwerking van persoonsgegevens in TOPdesk. Dit wordt weergegeven in de risicograaf die is ontwikkeld door de Britse toezichthouder ICO.

Tabel6 : Risicomatrix

Ernst van de impact	Ernstige impact	Laag risico **5, 6**	Hoog risico **2, 3, 7, 9, 10, 11, 12**	Hoog risico **1, 8**
	Enige impact	Laag risico	Gemiddeld risico	Hoog risico
	Minimale impact	Laag risico	Laag risico	Laag risico **4**
		Op afstand	Redelijke mogelijkheid	Waarschijnlijker wel dan niet
		Kans op schade		

Deel D: mitigerende maatregelen

Driving innovation together

Deel D beschrijft de voorgestelde (tegen)maatregelen die nodig zijn om de in deel C vastgestelde risico's te beperken. Dit deel bevat ook een analyse van het restrisico na de uitvoering van de voorgestelde maatregelen en een aanbeveling over de vraag of de maatregelen voldoende zijn om het risico tot een aanvaardbaar niveau te beperken.

2. Risicobeperkende maatregelen

2.1 Te nemen maatregelen om privacyrisico's te beperken

De onderstaande tabel toont de hoge gegevensbeschermingsrisico's voor betrokkenen, met de mitigerende maatregelen van de onderwijsinstelling en TOPdesk. De maatregelen voor de risico's die aanvankelijk al laag waren, zijn *cursief weergegeven*.

Tabel7 : Risicobeperkende maatregelen

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Risico na risicobeperking	Status van TOPdesk-maatregel
1.	Verlies van controle – gebrek aan beleid voor het reguleren van persoonsgegevens in de logbestanden van TOPdesk	Geen	Maak en implementeer een logbeleid waarin wordt beschreven welke persoonsgegevens op elk logniveau worden geregistreerd.	Laag	TOPdesk heeft een logbeleid opgesteld dat door alle afdelingen moet worden geïmplementeerd. De deadline hiervoor is het vierde kwartaal van 2026.
2.	Verlies van controle bij het sluiten van contracten op basis van het TOPdesk-sjabloon verwerkersovereenkomst – gebruik van optionele subverwerkers van TOPdesk	Zorg ervoor dat de verwerkersovereenkomst tussen de instelling en TOPdesk een weerspiegeling is van de subverwerkers die daadwerkelijk worden ingeschakeld.	Definieer optionele subverwerkers in de tabel op de SaaS-website.	Laag	Sinds 06-10-2025 vermeldt de SaaS-informatiepagina van TOPdesk welke subverwerkers optioneel zijn en informeert het klanten dat ze de toepasselijke subverwerkers kunnen vinden in hun hoofdovereenkomst. Door deze

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Risico na risicobeperking	Status van TOPdesk-maatregel
					geïmplementeerde maatregel is het risico nu laag.
3.	Verlies van controle – Actief abonnement vereist voor updates over de subverwerkers van TOPdesk	Geen	Alle verwerkingsverantwoordelijken actief informeren over wijzigingen in subverwerkers en voor elke wijziging toestemming vragen.	Laag	Op 09-10-2025 heeft TOPdesk zijn beleid aangepast. Nu ontvangen alle geregistreerde SaaS-hoofdcontactpersonen standaard een melding van een nieuwe subverwerker. Door deze geïmplementeerde maatregel is het risico nu laag.
4.	Verlies van controle – Overdracht van persoonsgegevens via Cloudflare niet weergegeven in verwerkersovereenkomst	*Zorg ervoor dat de doorgifte van persoonsgegevens via Cloudflare correct wordt weergegeven in de verwerkersovereenkomst en voldoet aan hoofdstuk V van de AVG.*	*Wijzig de TOPdesk-sjabloon verwerkersovereenkomst om de doorgifte van persoonsgegevens naar Cloudflare weer te geven*	Laag	Dit risico is al laag, dus er zijn geen maatregelen verplicht. TOPdesk zal deze maatregel echter in het eerste kwartaal van 2026 implementeren.

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Risico na risicobeperking	Status van TOPdesk-maatregel
5.	Verlies van controle – inzageverzoeken van buiten de EER bij Cloudflare	*Geen*	*Monitor mogelijke openbaarmakingen*	Laag	Dit risico is laag, dus er zijn geen maatregelen verplicht. TOPdesk blijft echter mogelijke openbaarmakingen door Cloudflare monitoren.
6.	Verlies van controle – doorgifte van persoonsgegevens via Microsoft	*Geen*	*Mogelijke openbaarmakingen in de gaten houden*	Laag	Dit risico is laag, dus er zijn geen maatregelen verplicht. TOPdesk blijft echter mogelijke openbaarmakingen door Microsoft monitoren.
7.	Verlies van controle – Automatische anonimisering mislukt voor derde betrokkenen	Implementeer een van de volgende maatregelen of een combinatie daarvan: • Een beleid om geen persoonsgegevens over derden op te nemen in de vrije tekstvelden van een kaart • Een beleid om de vrije tekstvelden van een kaart handmatig te anonimiseren • Een beleid om kaarten niet te anonimiseren, maar	Geen	Laag	Niet van toepassing

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Risico na risicobeperking	Status van TOPdesk-maatregel
		te verwijderen na hun bewaartermijn			
8.	Onvermogen om de rechten van de betrokkene uit te oefenen – Niet-tijdige hulp van Cloudflare en Microsoft	Geen	Implementeer een procedure om persoonlijke gegevens uit de logbestanden van Cloudflare te verstrekken.	Laag	Op 17-09-2025 heeft TOPdesk een procedure geïmplementeerd voor het verstrekken van persoonsgegevens uit de logbestanden van Cloudflare. Door deze maatregel is het risico nu laag.
9.	Onvermogen om rechten van betrokkenen uit te oefenen – Gegevens onzichtbaar voor beller	Procedure implementeren om onzichtbare antwoorden op te nemen in de antwoorden op verzoeken van betrokkenen.	Geen	Laag	Op 18-11-2025 heeft TOPdesk de noodzaak om deze procedure te implementeren toegevoegd aan de best practices in de kennisbank.
Maatregelen voor instellingen die bijzondere categorieën persoonsgegevens verwerken met TOPdesk					
#	**Risico**	**Maatregelen Instelling**	**Maatregelen TOPdesk**	**Risico na mitigatie**	**Status van TOPdesk-maatregel**

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Risico na risicobeperking	Status van TOPdesk-maatregel
10.	Verlies van vertrouwelijkheid en onrechtmatige verdere verwerking – Gebruik van bijzondere categorieën persoonsgegevens in test- of stagingomgeving	Maak gebruik van de optie om databasequery's uit te voeren om persoonsgegevens uit de productieomgeving te vervangen door synthetische gegevens voordat de gegevens naar een test- of stagingomgeving worden gekopieerd	Bied de mogelijkheid om automatisch het tabblad 'Privé' en 'Contract' van de kaarten te verwijderen bij het overzetten van productiegegevens naar een test- of stagingomgeving.	Laag	TOPdesk heeft aangegeven dat ze bezig zijn met de implementatie van deze maatregel. De deadline is Q2 2026. Daarnaast heeft TOPdesk op 18-11-2025 aan de best practices in de kennisbank toegevoegd dat deze procedure moet worden geïmplementeerd.
11.	Verlies van controle – Verwerking van bijzondere categorieën persoonsgegevens in TOPdesk	Voer de juiste compliance-werkzaamheden uit voordat u bijzondere categorieën persoonsgegevens in TOPdesk verwerkt, om ervoor te zorgen dat de instelling een beroep kan doen op een van de uitzonderingen in artikel 9, lid 2, van de AVG. Zorg ervoor dat bij het verwerken van bijzondere categorieën persoonsgegevens in TOPdesk dit correct wordt weergegeven in de	Maak of update een kennisitem voor instellingen met informatie en best practices over de verwerking van bijzondere categorieën gegevens in TOPdesk.	Laag	TOPdesk verwacht dat deze maatregel tegen het einde van het vierde kwartaal van 2025 is geïmplementeerd.

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Risico na risicobeperking	Status van TOPdesk-maatregel
		verwerkersovereenkomst met TOPdesk.			
		Configureer geen (medische) aandoeningen in Attenties, maar relevante acties die een operator moet ondernemen.			
		Maak bij het registreren van bijzondere categorieën persoonsgegevens van een betrokkene gebruik van het tabblad 'Privé' op de persoonskaart in de module Ondersteunende bestanden (zie §**Fout! Verwijzingsbron niet gevonden.**).			
12.	Verlies van controle – onvoldoende auditlogging van bijzondere categorieën gegevens	Bij gebrek aan implementatie door TOPdesk van aanvullende logging bij toegang tot en wijziging van het tabblad Privé: Implementeer auditlogging bij toegang tot kaarten van processen die waarschijnlijk bijzondere categorieën gegevens bevatten.	Implementeer aanvullende auditlogging: log wie welke kaart wanneer heeft geopend en voeg deze optie toe aan aangepaste logacties.	Laag	TOPdesk zal standaard aanvullende logging implementeren voor toegang tot en wijziging van het privétabblad op de persoonskaart. Dit staat gepland voor het eerste kwartaal van 2026.
		Nadat TOPdesk aanvullende logging heeft geïmplementeerd voor			

#	Risico	Maatregelen Instelling	Maatregelen TOPdesk	Risico na risicobeperking	Status van TOPdesk-maatregel
		toegang tot en wijziging van het privétabblad: maak gebruik van het privétabblad op persoonskaarten om speciale categorieën gegevens te verwerken.			

2.2 Beoordeling van het risico na maatregelen

Als een van de restrisico's na implementatie van de mitigerende maatregelen 'hoog' is, is voorafgaand overleg met de gegevensbeschermingsautoriteit verplicht. Op basis van de analyse blijven er na implementatie van de mitigerende maatregelen alleen lage restrisico's over. Daarom is voorafgaand overleg niet nodig.

3. Conclusie

Deze DPIA heeft negen hoge risico's en drie lage risico's voor de rechten en vrijheden van betrokkenen geïdentificeerd.

Deze risico's zijn deels te wijten aan de manier waarop instellingen TOPdesk (waarschijnlijk) zullen gebruiken, en deels aan het ontwerp van TOPdesk zelf. Drie van de hoge risico's houden verband met de mogelijkheid dat een instelling bijzondere categorieën persoonsgegevens verwerkt in TOPdesk; als een instelling dit niet doet, zijn deze drie risico's niet van toepassing. Voor alle risico's, inclusief de drie lage risico's, zijn maatregelen voorgesteld. Zeven van deze maatregelen zijn van toepassing op instellingen en tien op TOPdesk.

Door deze maatregelen te implementeren worden alle hoge risico's beperkt, waardoor alleen lage restrisico's overblijven. In dat geval is voorafgaand overleg met de Autoriteit Persoonsgegevens niet nodig. Hoewel het niet strikt noodzakelijk is om lage risico's te beperken, wordt dit wel aanbevolen omdat de maatregelen relatief eenvoudig te implementeren zijn en de rechten en vrijheden van betrokkenen versterken.

> **Update 12/12/2025:** Terwijl de DPIA werd uitgevoerd, heeft TOPdesk al verschillende maatregelen genomen om de geïdentificeerde risico's te beperken. Meer specifiek heeft TOPdesk al maatregelen genomen voor vier hoge risico's (#2, 3, 8, 9) en maatregelen geïmplementeerd voor alle lage risico's. Voor één hoog risico zijn alleen maatregelen van de instelling nodig. Op het moment van schrijven blijven er dus vier hoge risico's over. Voor al deze risico's is een tijdschema voor de implementatie van de maatregelen opgesteld. Instellingen kunnen dus gewoon doorgaan met het gebruik. Als de resterende hoge risico's worden beperkt, is voorafgaand overleg met de gegevensbeschermingsautoriteit niet nodig. SURF zal in 2026 een update over deze DPIA publiceren met een conclusie over de implementatie van de resterende maatregelen.