Driving innovation together

DPIA HR2day

Applicatie voor personeelszaken en salarisadministratie

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

Auteur(s): Sophia Gelpke & Jan Landsaat
Versie: 1.0
Datum: 12 mei 2026

Samenvatting

Dit rapport is een gegevensbeschermingseffectbeoordeling (hierna: DPIA) met betrekking tot het gebruik van de SaaS-applicatie HR2day door Nederlandse onderwijsinstellingen (hierna: instellingen), aangeboden door HR2day B.V. (hierna: HR2day). Deze DPIA is een referentie-DPIA, uitgevoerd door sectororganisatie SURF, die instellingen een algemeen kader biedt voor het beoordelen van gegevensbeschermingsrisico's binnen HR2day.

Over de dienst
HR2day is een veelzijdig systeem voor personeelszaken en salarisadministratie (hierna: HR) dat bestaat uit verschillende modules en het volledige traject van een medewerker ondersteunt, van onboarding tot offboarding en alles daartussenin. Het biedt standaardprocessen die kunnen worden aangepast aan het gebruik van individuele instellingen en wordt gebruikt door zowel beroepsopleidingen als hogescholen. Als cloudgebaseerde SaaS-applicatie is HR2day specifiek gebouwd om op het Salesforce-platform te draaien, waarbij gebruik wordt gemaakt van kerntechnologieën en -diensten van Salesforce om een schaalbare HR-ervaring te bieden.

Reikwijdte
SURF heeft zowel juridisch als technisch onderzoek verricht om algemene gegevensbeschermingsrisico's in kaart te brengen die voortvloeien uit de gegevensverwerkingsactiviteiten die instellingen in HR2day uitvoeren. De geteste modules zijn:

- Personeels- en salarisadministratie
- Selfservice (ESS/MSS)
- Verlof
- Verzuim
- Onkostendeclaraties
- Documentbeheer
- Rapporten
- Digitale handtekening
- HR-analyses
- Feedback van medewerkers
- Arbokoppeling (API)

Daarnaast heeft SURF de mobiele applicatie HR2day+ beoordeeld.

Aangezien dit een referentie-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 algemene beoordeling gedaan op basis van het beoogde gebruik van HR2day door instellingen. Instellingen die HR2day willen gebruiken, kunnen deze DPIA als uitgangspunt nemen, maar moeten deze aanvullen, uitbreiden en/of aanpassen op basis van de specifieke context waarin zij van plan zijn HR2day willen gebruiken.

Methodologie
SURF heeft de volgende methoden gebruikt om de beoordeling uit te voeren:

- Bureau-onderzoek en juridische beoordeling van de contracten, certificeringen en andere documentatie van HR2day.
- Vragenlijsten aan de vertegenwoordigers van HR2day.
- Technisch onderzoek in de browsergebaseerde applicatie, uitgevoerd in een testomgeving die HR2day voor SURF heeft opgezet, waarbij gebruik is gemaakt van een gespecialiseerde monitoringtool (man-in-the-middle-proxy).
- Verzoeken om inzage van betrokkenen, ingediend na het technische onderzoek.
- Reviews door TOPdesk en SURF.

Resultaat: 16 hoge risico's en 2 risico's waarvan het niveau nog moet worden bepaald
Deze DPIA heeft zestien hoge risico's voor betrokkenen geïdentificeerd en twee risico's waarvan het risiconiveau nog moet worden bepaald. Vijf van de hoge risico's houden verband met het gebruik van Salesforce als aanbieder van het platform waarop HR2day draait. Elf van de hoge risico's zijn algemene risico's, veroorzaakt door de manier waarop instellingen HR2day (waarschijnlijk) gebruiken of door het ontwerp van HR2day. Twee van de risico's houden verband met het gebruik van de mobiele app. Deze twee risico's bestaan voor elke app die gebruikmaakt van de app store en pushmeldingen. Aangezien SURF een aanvullend onderzoek uitvoert naar de impact van deze risico's, zal het risiconiveau op een later tijdstip worden bepaald.

Door onderstaande maatregelen te implementeren worden alle hoge risico's gemitigeerd, waardoor alleen lage restrisico's overblijven. Hoewel het niet strikt noodzakelijk is om lage risico's te mitigeren, wordt dit wel aanbevolen.

Voor al deze risico's is er een tijdschema voor de implementatie van de maatregelen. Daarom kunnen instellingen HR2day blijven gebruiken. Als de hoge risico's worden gemitigeerd, is voorafgaand overleg met de gegevensbeschermingsautoriteit niet vereist. SURF zal in 2027 een update over deze DPIA publiceren met een conclusie over de implementatie van de resterende maatregelen.

Een overzicht van alle geïdentificeerde risico's en voorgestelde maatregelen is weergegeven in de onderstaande tabel. De status van de door HR2day te nemen maatregelen is weergegeven in de rechterkolom.

#	Risico	Maatregelen instelling	Maatregelen HR2day	Status van de maatregel(en) van HR2day
Risico's met betrekking tot het Salesforce-platform				
16.1	Verlies van controle en vertrouwelijk-heid door ongeoorloofd e toegang via doorgifte	Neem alle rechtmatige doorgiften op in de verwerkers-overeenkomst	Neem alle rechtmatige doorgiften op in de verwerkersovereenk omst	De deadline hiervoor is 31-12-2026.

	naar Salesforce			
16.2	Verlies van controle als gevolg van een gebrek aan transparantie over de verwerking van gebruiks-gegevens voor doeleinden Salesforce	Werk de verwerkersovereen komst tussen HR2day en instellingen bij met: alle categorieën persoonsgegevens, inclusief gebruiksgegevens indien van toepassing, die HR2day en subverwerkers namens instellingen verwerken; legitieme zakelijke doeleinden waarvoor en onder welke voorwaarden HR2day en subverwerkers persoonsgegevens mogen verwerken; doeleinden waarvoor HR2day en subverwerkers geen persoonsgegevens mogen verwerken;	Update verwerkersovereenk omst tussen HR2day en instellingen met: alle categorieën persoonsgegevens, inclusief gebruiksgegevens indien van toepassing, die HR2day en subverwerkers namens instellingen verwerken; legitieme zakelijke doeleinden waarvoor en onder welke voorwaarden HR2day en subverwerkers persoonsgegevens mogen verwerken; doeleinden waarvoor HR2day en subverwerkers geen persoonsgegevens mogen verwerken; auditrecht voor instellingen met betrekking tot de verwerkersovereenk omst.	De deadline hiervoor is 31-12-2026.

		auditrecht voor instellingen met betrekking tot de verwerkersovereen komst.	Update verwerkersovereenk omst tussen HR2day en Salesforce met: alle categorieën persoonsgegevens, inclusief gebruiksgegevens indien van toepassing, die Salesforce namens instellingen verwerkt; legitieme zakelijke doeleinden waarvoor en onder welke voorwaarden Salesforce persoonsgegevens mag verwerken; doeleinden waarvoor Salesforce geen persoonsgegevens mag verwerken; auditrecht voor instellingen met betrekking tot de verwerkersovereenk omst.	De deadline hiervoor is 31-12-2026.
16.3	Onvermogen om de inzagerechte n van betrokkenen tot persoonsgeg evens uit te oefenen		Verbeter het DSAR-beleid zodat HR2day volledige toegang kan bieden tot alle persoonsgegevens die zij en hun subverwerkers verwerken.	HR2day zal zijn eigen DSAR-beleid uiterlijk op 1 augustus 2026 aanpassen. Toegang tot mogelijke persoonsgegevens in Salesforce is afhankelijk van de implementatie van de maatregelen voor risico 16.2.
16.4	Verlies van controle door gebrek aan transparantie		Zorg voor een volledige cookieverklaring voor alle gebruikers	HR2day zal de cookieverklaring uiterlijk op 1-8-2026 voltooien en de

	over de verwerking van persoonsgegevens via cookies		die HR2day gebruiken.	cookieverklaring opnemen in hun jaarkalender.
16.5	Verlies van controle doordat men zich moet registreren voor updates van subverwerkers van Salesforce		Implementeer een proces waarbij HR2day de subverwerkers van Salesforce aan instellingen communiceert.	De deadline hiervoor is 31-12-2026 (afhankelijk van maatregelen voor risico 16.2).
Algemene risico's				
16.6	Verlies van controle door een gebrek aan transparantie over de verwerking van persoons-gegevens voor doeleinden van HR2day	Werk de verwerkersovereen komst tussen HR2day en instellingen bij met: alle categorieën persoonsgegevens, inclusief gebruiksgegevens indien van toepassing, die HR2day en subverwerkers namens instellingen verwerken; legitieme zakelijke doeleinden waarvoor en onder welke voorwaarden HR2day en subverwerkers persoonsgegevens mogen verwerken; doeleinden waarvoor HR2day en subverwerkers	Update verwerkersovereenk omst tussen HR2day en instellingen met: alle categorieën persoonsgegevens, inclusief gebruiksgegevens indien van toepassing, die HR2day en subverwerkers namens instellingen verwerken; legitieme zakelijke doeleinden waarvoor en onder welke voorwaarden HR2day en subverwerkers persoonsgegevens mogen verwerken; doeleinden waarvoor HR2day en subverwerkers geen persoonsgegevens mogen verwerken; auditrecht voor instellingen met	De deadline hiervoor is 31-12-2026.

		geen persoonsgegevens mogen verwerken; auditrecht voor instellingen met betrekking tot de verwerkersovereen komst.	betrekking tot de verwerkersovereenk omst.	
			Update privacyverklaring HR2day.	HR2day zal haar privacyverklaring uiterlijk op 1-8-2026 bijwerken.
16.7	Verlies van controle over gegevens over gebruikers-tevredenheid		Neem deze verwerking op in de verwerkersovereenk omst met HR2day als verwerker en geef instellingen zinvolle controle (door middel van transparantie) en keuzes bij deze verwerking.	HR2day zal dit uiterlijk op 31-12-2026 in de verwerkersovereenk omst opnemen en instellingen de mogelijkheid bieden deze functionaliteit uit te schakelen.
16.8	Verlies van controle en vertrouwelijk heid door ongeoorloofd e toegang in derde landen	Stop met het gebruik van SignRequest	Identificeer alle overdrachten, in ieder geval naar Expo en Google	De deadline hiervoor is 31-12-2026.
			Neem rechtmatige doorgiften aan subverwerkers op in de verwerkersovereenk omst tussen HR2day en de instelling.	De deadline hiervoor is 31-12-2026.

			Informeer instellingen over de partijen waaraan persoonsgegevens worden doorgegeven en waarmee zij rechtstreeks overeenkomsten moeten sluiten .	De deadline hiervoor is 31-12-2026.
			Zorg ervoor dat klanten die stoppen met het gebruik van SignRequest een kopie kunnen krijgen van de verwerkte gegevens van hun betrokkenen en deze indien nodig kunnen verwijderen.	SignRequest verwijdert de omgeving van een klant, inclusief de persoonsgegevens, al een maand nadat de klant is gestopt met het gebruik van hun diensten. HR2day zal uiterlijk op 31-12-2026 verifiëren dat deze verwijdering alle persoonsgegevens van de betrokkenen van instellingen omvat en dat instellingen een kopie van de persoonsgegevens kunnen verkrijgen.
16.9	Verlies van controle over subverwerkers en ontvangers door ontbrekende of onjuiste overeenkomsten		Voer een beoordeling uit of Google en Apple kwalificeren als subverwerkers, gezamenlijke verwerkingsverantwoordelijken of externe ontvangers.	De deadline hiervoor is 31-12-2026.
			Neem Google en Apple op in de verwerkersovereenkomst tussen HR2day en de instellingen.	De deadline hiervoor is 31-12-2026.

			Sluit de benodigde overeenkomsten met Google en Apple.	De deadline hiervoor is 31-12-2026. HR2day streeft ernaar om uiterlijk op 1-8-2026 subverwerkersovereenkomsten te hebben gesloten met alle subverwerkers.
16.10	Verlies van vertrouwelijkheid door het ontbreken van 'read access logging'	Implementeer 'read access logging' op ten minste de categorieën gevoelige en bijzondere gegevens.	Schakel 'read access logging' in voor categorieën gevoelige en bijzondere gegevens en voor de proxy-inlogfunctionaliteit.	HR2day stelt logboekregistratie van leestoegang beschikbaar voor instellingen op 31-12-2026. Daarnaast start HR2day een werkgroep met instellingen.
		Implementeer logboekregistratie van leestoegang voor activiteiten die beheerders uitvoeren via de proxy-login.		
		Gebruikers onverwijld informeren dat er misbruik is gemaakt van hun identiteit.		
16.11	Schending van het beginsel van minimale gegevensverwerking door het opnemen van te brede lijsten met redenen voor afwezigheid	Gebruik uitsluitend keuzelijsten om informatie te verzamelen over de reden van de afwezigheid van medewerkers en een vaste reeks velden om aanvullende informatie over hun afwezigheid te verzamelen.	Geef instellingen instructies over het gebruik van keuzelijsten voor het verzamelen van gevoelige en bijzondere categorieën gegevens.	HR2day geeft aan dit in zijn ontwikkelingscyclus te hebben geïmplementeerd en heeft laten zien hoe het gebruikers waarschuwt om geen informatie over de aard en oorzaak van de afwezigheid op te nemen. De deadline

		Laat de keuzelijst voor verzuim en de vaste set velden beoordelen door de privacyafdeling, om er zeker van te zijn dat ze in overeenstemming zijn met de AVG-vereisten en de beschikbare richtlijnen.		voor deze maatregel is 31-12-2026.
		Zorg ervoor dat gebruikers van HR2day goed worden geïnstrueerd en getraind over welke soorten gegevens mogen worden verwerkt met betrekking tot de afwezigheid van werknemers.		
16.12	Gebrek aan juistheid door handmatige registratie van persoonsgegevens	Gebruik open tekstvelden alleen met een duidelijk doel.	Geef instellingen instructies over het gebruik van open tekstvelden op een manier die de beginselen van minimale gegevensverwerking respecteert.	HR2day geeft aan dit in de ontwikkelingscyclus te hebben geïmplementeerd. HR2day waarschuwt voor voorzichtigheid bij het gebruik van samenvoegvelden die gevoelige gegevens bevatten in het scherm voor het instellen van waarschuwingen. De deadline voor deze maatregel is 31-12-2026.
		Formuleer vragen op een manier die duidelijk maakt welke	Bied voldoende opties voor veldvalidatie om onjuiste	HR2day geeft aan dit in de ontwikkelingscyclus te hebben

		(gevoelige/bijzondere) persoonsgegevens wel en niet in een open tekstveld moeten worden ingevuld en maak gebruik van de beschikbare informatiepictogrammen.	gegevensverwerking te voorkomen.	geïmplementeerd en veldvalidatie te tonen voor BSN-nummers en IBAN's. De deadline voor deze maatregel is 31-12-2026.
		Zorg ervoor dat gebruikers van HR2day goed worden geïnstrueerd en getraind over welke soorten gegevens in open tekstvelden mogen worden verwerkt.		
16.13	Gebrek aan juistheid door handmatige registratie van persoonsgegevens	Automatiseer de invoer waar mogelijk, bijvoorbeeld door HR2day te koppelen aan het wervingssysteem.	Zorg voor voldoende mogelijkheden voor veldvalidatie om onnauwkeurige gegevensverwerking te voorkomen.	HR2day geeft aan dit in de ontwikkelingscyclus te hebben geïmplementeerd en toont veldvalidatie voor bsn-nummers en IBAN's. De deadline voor deze maatregel is 31-12-2026.
		Zorg ervoor dat HR-medewerkers goed zijn geïnstrueerd en getraind in de procedures van de instellingen voor het zorgvuldig registreren van persoonsgegevens.		
16.14	Verlies van controle over bewaartermijnen door gebrek aan	Bepaal en beheer bewaartermijnen voor persoonsgegevens in HR2day.	Geef instellingen informatie en instructies over de procedure voor het verwijderen van gegevens met	HR2day heeft contact met twee instellingen en werkt aan (i) het gewenste detailniveau van bewaartermijnen

	automatisering		behulp van signaallijsten.	(generiek versus per gegevensgroep) en (ii) de mate van uniformiteit tussen instellingen. De deadline voor deze maatregelen is 31-12-2026.
		Zorg ervoor dat de bewaartermijnen worden nageleefd door processen in te voeren om deze af te dwingen, bijvoorbeeld door gebruik te maken van de geautomatiseerde bewaartermijnen voor documenten.	Ondersteun instellingen bij het handhaven van hun bewaartermijnen door de mogelijkheden voor technische configuratie en beheer van bewaartermijnen per groep persoonsgegevens in HR2day te verbeteren.	
16.15	Verlies van vertrouwelijkheid door standaardinstelling voor verticale overerving van rechten	Schakel de verticale overerving van rechten uit, tenzij het nodig is om deze instelling te gebruiken.	Informeer instellingen proactief over de privacyimplicaties van de instelling voor verticale overerving van rechten en bied hen de keuze om deze in of uit te schakelen.	De deadline hiervoor is 31-12-2026.
		Beperk de toegang tot persoonsgegevens voor functies die deze gegevens niet nodig hebben om hun taken uit te voeren.	Werk samen met instellingen om de mogelijkheden te verbeteren om het beginsel van minimale gegevensverwerking te respecteren terwijl de instelling voor verticale overerving van rechten is ingeschakeld, waardoor de administratieve lasten worden verminderd, OF stel hen in staat de noodzakelijke	
		Wees transparant tegenover de betrokkenen over het gebruik van de instelling voor verticale overerving van rechten en over wie toegang heeft tot hun gegevens.		

			workflows uit te voeren terwijl de instelling is uitgeschakeld.	
16.16	Verlies van vertrouwelijkheid door gebrek aan beheer van encryptie-sleutels	Beoordeel of encryptie op celniveau, encryptie met door de klant beheerde sleutels en eventuele andere aanvullende maatregelen noodzakelijk zijn voor bijzondere en gevoelige categorieën gegevens, rekening houdend met de specifieke gegevens die door de instelling worden verwerkt en de andere beveiligingsmaatregelen die van kracht zijn.	Informeer instellingen over de encryptiesmethoden die worden gebruikt voor de HR2day-applicatie en het platform en over de mogelijkheid van aanvullende waarborgen, zoals encryptie op celniveau en door HR2day beheerde encryptiessleutels.	Op 31-12-2026 zal HR2day aanvullende beveiligingsmaatregelen voor instellingen beschikbaar stellen. De mogelijkheid voor instellingen om hun eigen encryptiessleutels te beheren bestaat al. Daarnaast zal HR2day samen met instellingen een werkgroep opzetten om de gewenste opties te beoordelen.
			Samenwerken met instellingen bij het beoordelen van het vereiste encryptiesniveau voor de persoonsgegevens in HR2day, met name voor de gevoelige en bijzondere categorieën persoonsgegevens.	
			Waar instellingen dit nodig achten, worden aanvullende beveiligingsmaatregelen geïmplementeerd, zoals encryptie op celleniveau en encryptiessleutels die door HR2day worden beheerd.	
Risico's van mobiele apps				

16.17	Verlies van controle over de verwerkte persoonsgegevens door de installatie van de mobiele app via een app-store van een derde partij	Maak toegang via de mobiele browser vanaf mobiele apparaten mogelijk.	Maak de app beschikbaar als sideload.	HR2day zal contact opnemen met instellingen over hun wensen in dit verband.
		Voer evenredigheids- en subsidiariteitsbeoordelingen uit met betrekking tot het aanbieden van de mobiele app via app-winkels en 'side-loading' en implementeer de resultaten.	Maak toegang via de mobiele browser vanaf mobiele apparaten mogelijk.	HR2day zal contact opnemen met instellingen over hun wensen hieromtrent.
16.18	Verlies van controle door verwerking van pushmelding en door Google en Apple	Neem geen persoonsgegevens op in de berichten die via pushmeldingen worden verzonden.	Optioneel: Implementeer Unified Push voor Android-gebruikers.	HR2day zal geen stappen ondernemen voor deze optionele maatregel.
		Voer evenredigheids- en subsidiariteitsbeoordelingen uit met betrekking tot het verzenden van pushmeldingen via Google en Apple of Unified Push en implementeer de resultaten.		

Deel C Beschrijving van risico’s

Dit deel betreft de beschrijving en beoordeling van de risico’s voor betrokkenen. Dit zijn de risico’s zoals die zijn vastgesteld tijdens het testen en analyseren en vóór het nemen van risicobeperkende maatregelen. De risico's worden vervolgens ingedeeld op basis van de waarschijnlijkheid dat ze zich voordoen en de impact op 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 noemt de volgende hoofdcategorieën van risico's:

- het onvermogen om rechten uit te oefenen (met inbegrip van, maar niet beperkt tot, privacyrechten);
- het onvermogen om toegang te krijgen tot diensten of kansen;
- 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 significante economische of sociale nadelen.

Deze hoofdcategorieën bieden houvast bij het vaststellen 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 risicografiek die is ontwikkeld door de Britse toezichthouder ICO, als volgt:

Tabel: ICO-risicomodel

Ernst van de impact	Ernstige impact	Laag risico	Hoog risico	Hoog risico
	Enige impact	Laag risico	Gemiddeld risico	Groot risico
	Minimale impact	Laag risico	Laag risico	Laag risico
		Heel klein	Redelijke kans	Waarschijnlijker dan niet
		Waarschijnlijkheid/kans op schade		

In deze DPIA worden de volgende betekenissen van de "waarschijnlijkheid van schade" en de "ernst van de gevolgen" gebruikt om de risico's te beoordelen:

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

Impact	**Betekenis**
Minimale gevolgen	De gevolgen voor de betrokkene hebben weinig of geen invloed op de rechten en vrijheden van de betrokkene wanneer het risico zich voordoet
Enige negatieve gevolgen	De gevolgen voor de betrokkene hebben een beperkte impact op de rechten en vrijheden van de betrokkene wanneer het risico zich voordoet
Ernstige negatieve gevolgen (ernstige impact)	De gevolgen voor de betrokkene hebben een aanzienlijke impact op de rechten en vrijheden van de betrokkene wanneer het risico zich voordoet

16 Risico's

Salesforcerisico's

16.1 Verlies van controle en vertrouwelijkheid door ongeoorloofde toegang door doorgiftes aan Salesforce

HR2day zorgt ervoor dat Salesforce de klantgegevens host in datacenters binnen de EER. De overdrachten die plaatsvinden doordat Salesforce als verwerker optreedt, worden beschreven in de paragrafen over**Fout! Verwijzingsbron niet gevonden.** en**Fout! Verwijzingsbron niet gevonden.** .

Salesforce is een in de VS gevestigd bedrijf, wat betekent dat het onder de werkingssfeer van de Amerikaanse wetgeving valt. Daarom bestaat, zoals beschreven in **Fout! Verwijzingsbron niet gevonden.Fout! Verwijzingsbron niet gevonden.,** de kans dat Salesforce wettelijk verplicht is om persoonsgegevens aan Amerikaanse autoriteiten te verstrekken op basis van Amerikaanse wetgeving, zoals de CLOUD-wet. Aangezien Salesforce het beheer van de encryptiesleutels verzorgt, kunnen de betreffende gegevens bestaan uit gedecodeerde persoonsgegevens in klantgegevens, loggegevens en IP-adressen van betrokkenen, evenals alle persoonsgegevens in de gebruiksgegevens van Salesforce. De gegevensverwerkingsovereenkomst tussen Salesforce en HR2day verplicht Salesforce om HR2day op de hoogte te stellen van en door te sturen naar verzoeken van derden om persoonsgegevens openbaar te maken, dergelijke verzoeken aan te vechten en betrokkenen schadeloos te stellen in het geval dat persoonsgegevens zijn overgedragen – voor zover dit wettelijk is toegestaan. De overeenkomst bevat echter geen canary-clausule die hen verplicht om een instelling op de hoogte te stellen van hun onvermogen om aan hun contractuele verplichtingen te voldoen indien zij een verzoek ontvangen dat vergezeld gaat van een spreekverbod.

Bovendien biedt Salesforce ondersteuningsdiensten aan zoals beschreven op **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** en **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** , wat betekent dat personeel uit vijf derde landen toegang zou kunnen krijgen tot gegevens van de klantondersteuning en databasetabellen. Er zijn organisatorische en technische maatregelen getroffen om deze toegang tot een minimum te beperken en ervoor te zorgen dat, mocht er toch toegang plaatsvinden, de negatieve gevolgen zo klein mogelijk blijven.

Ten slotte kunnen, zoals beschreven in **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** en **Fout! Verwijzingsbron niet gevonden.Fout! Verwijzingsbron niet gevonden.**, inlogverzoeken buiten de EU worden opgeslagen (hoewel HR2day aangeeft deze functionaliteit niet te gebruiken) en maakt Salesforce gebruik van een CDN.

Uit het transparantierapport van Salesforce blijkt dat het eerder verzoeken om zowel inhoudelijke als niet-inhoudelijke gegevens heeft ontvangen en hieraan heeft voldaan. De beschreven bestaande maatregelen voor de gegevensoverdrachten in combinatie met het bestaan van de beschermingsmaatregelen van het Data Privacy Framework (dat ook bescherming biedt voor verdere doorgifte), de BCR-P van Salesforce en de SCC's betekenen

echter dat, zolang het Data Privacy Framework bestaat, de kans op een negatieve impact voor betrokkenen zeer klein is. Dit vereist wel dat alle overdrachten correct worden vastgelegd in de verwerkersovereenkomst tussen instellingen en HR2day, zodat deze wettelijke beschermingsmaatregelen van toepassing zijn op de overdrachten. Wanneer ze niet worden vastgelegd, is de kans op schade waarschijnlijker wel dan niet, aangezien deze beschermingsmaatregelen dan niet van toepassing zijn. Wanneer er sprake is van ongeoorloofde toegang of openbaarmaking, leidt dit tot een verlies van controle voor de betrokkenen, wat ernstige impact aan hun rechten en vrijheden kan veroorzaken. Hun (gevoelige of bijzondere categorieën van) persoonsgegevens zouden bijvoorbeeld voor onbekende doeleinden (zoals surveillance) kunnen worden verwerkt, zonder dat er een mogelijkheid tot verhaal bestaat. Dit risico is momenteel dus laag voor instellingen die de gegevensoverdrachten naar Salesforce hebben vastgelegd, en hoog voor instellingen die dat niet hebben gedaan.

16.2 Verlies van controle als gevolg van een gebrek aan transparantie over de verwerking van gebruiksgegevens voor doeleinden Salesforce

In de privacyverklaring van Salesforce staat vermeld dat Salesforce via logbestanden en andere technologieën informatie over de apparaten van gebruikers en hun gebruik van de diensten van Salesforce kan verwerken. Deze privacyverklaring is van toepassing op alle diensten van Salesforce, inclusief het platform van HR2day. Hierin wordt uitgesloten dat Salesforce klantgegevens voor eigen doeleinden verwerkt, maar aangezien de subverwerkersovereenkomst alleen klantgegevens omvat, blijft de mogelijkheid bestaan dat Salesforce soorten gegevens verwerkt die niet in de verwerkersovereenkomst zijn opgenomen, zoals loggegevens en gebruiksgegevens. Salesforce beweert dat het gebruiksgegevens verwerkt op een manier die het niet mogelijk maakt om individuen te identificeren. SURF heeft geen verwerking van persoonsgegevens door Salesforce waargenomen zoals beschreven in de privacyverklaring, omdat SURF onder andere om technische redenen geen toegang heeft tot de verwerking door Salesforce. Daarom heeft SURF ook niet (technisch) kunnen verifiëren dat deze verwerking niet plaatsvindt, noch dit juridisch kunnen uitsluiten. Het is dus onduidelijk welke persoonsgegevens door Salesforce worden verzameld, voor welke doeleinden, wat de bewaartermijnen zijn en hoe Salesforce pseudonimisering- en anonimiseringstechnieken toepast. HR2day heeft geen uitputtende lijst kunnen verstrekken van de gegevensvelden die Salesforce in hun gebruiksgegevens verzamelt, noch een toelichting op hun anonimiseringstechnieken. SURF kan niet uitsluiten dat Salesforce de persoonsgegevens van de gebruikers van HR2day verwerkt op de manieren die in de privacyverklaring worden beschreven, inclusief de verdere verwerking voor eigen doeleinden, zoals serviceverbetering. Aangezien er geen verenibaarbaarheidstest is uitgevoerd en eventuele verdere verwerkingsactiviteiten niet zijn opgenomen in de verwerkersovereenkomsten, leidt de mogelijkheid van deze verdere verwerking tot een verlies van controle.

De kans dat er sprake is van een verlies van controle is waarschijnlijker wel dan niet, aangezien – ondanks de inspanningen van HR2day om deze informatie te verkrijgen – Salesforce onvoldoende garanties heeft kunnen bieden om de informatie in hun privacyverklaring te weerleggen. Dit veroorzaakt ernstige impact voor de betrokkenen, omdat de gegevensverwerking zoals beschreven in de privacyverklaring van Salesforce uitgebreid is, de betreffende gegevens gevoelig of bijzonder kunnen zijn en instellingen geen controle hebben over de verwerking van deze gegevens. Salesforce neemt in zijn

privacyverklaring ook verwerkingsdoeleinden op zoals het trainen van AI-modellen, een doel dat ver afstaat van de oorspronkelijke doeleinden van de instellingen bij de verwerking van hun HR- en salarisgegevens en niet in overeenstemming is met de redelijke verwachtingen van de betrokkenen. Bovendien betekent het gebrek aan transparantie dat instellingen niet kunnen voldoen aan de informatierechten van hun betrokkenen. Dit is daarom een hoog risico.

16.3 Onvermogen om de inzagerechten van betrokkenen op persoonlijke gegevens uit te oefenen

Het antwoord op het DSAR-verzoek aan HR2day was onvolledig. HR2day verstrekte wel de gegevens in de applicatie over de betrokkenen, de inloggeschiedenis en de mutatielogboeken. Echter, alle verdere logboekregistratie die HR2day uitvoert volgens de documentatie die zij verstrekten na hun DSAR-antwoord, namelijk de gebeurtenisbewaking, het audittraject van de configuratie en de e-maillogboeken, ontbrak in het DSAR-antwoord. Bovendien is er geen informatie verstrekt over de gebruiksgegevens die Salesforce als subverwerker verwerkt. Ook ontbraken de persoonsgegevens die worden verwerkt via subverwerkers Expo en SignRequest en mogelijke subverwerkers Google en Apple.

Dit brengt het risico met zich mee dat betrokkenen hun rechten op grond van de AVG niet effectief kunnen uitoefenen. De kans dat dit gebeurt, is groter dan dat het niet gebeurt, aangezien het daadwerkelijk is voorgekomen. Het niet halen van de termijn voor het verzoek om inzage, zelfs voor slechts een deel van de gegevens, leidt tot ernstige aantasting van de rechten van de betrokkene, aangezien het recht op inzage een grondrecht is. Dit risico is dan ook hoog.

16.4 Verlies van controle door gebrek aan transparantie over de verwerking van persoonsgegevens via cookies

HR2day heeft geen cookieverklaring waarin wordt gedocumenteerd welke cookies HR2day en haar subverwerkers (met name Salesforce) gebruiken om persoonsgegevens te verzamelen. Daardoor kunnen betrokkenen zich niet informeren over de verwerking die HR2day en haar subverwerkers via cookies uitvoeren voordat de verwerking begint, en kunnen zij hun rechten niet uitoefenen.

De kans dat dit gebeurt is waarschijnlijker wel dan niet, aangezien er op dit moment geen volledige cookieverklaring is. Dit brengt ernstige impact toe aan betrokkenen, aangezien zij hun rechten als betrokkene niet kunnen uitoefenen. Dit is daarom een hoog risico.

16.5 Verlies van controle doordat men zich moet registreren voor updates over subverwerkers van Salesforce

Om op de hoogte te worden gesteld van nieuwe subverwerkers van Salesforce, moeten resellers en klanten zich via hun formulier registreren voor updates. Sommige medewerkers van HR2day zijn geregistreerd voor deze updates, maar er is geen bekend proces om instellingen te informeren over nieuwe subverwerkers, zodat instellingen hun rechten uit de verwerkersovereenkomst kunnen uitoefenen. Het niet informeren van instellingen over nieuwe subverwerkers zou een schending van hun verwerkersovereenkomsten inhouden.

De kans dat dit gebeurt is redelijk groot, aangezien er geen garantie is dat instellingen op de hoogte worden gesteld van nieuwe subverwerkers. Zonder de juiste informatie bevinden betrokkenen zich niet in een positie waarin zij hun rechten als betrokkenen effectief kunnen uitoefenen, wat leidt tot een verlies van controle dat ernstige impact veroorzaakt. Het algehele risico is hoog.

Algemene risico's

16.6 Verlies van controle door een gebrek aan transparantie over de verwerking van persoonsgegevens voor doeleinden van HR2day

In de verklaring van HR2day staat dat HR2day gegevens over gebruikers mag verzamelen en verwerken voor eigen doeleinden, zoals het verbeteren van hun diensten. Uit de bewoordingen van deze verklaring blijkt niet duidelijk of HR2day hiervoor persoonsgegevens gebruikt die het als verwerker heeft verkregen. Dit gebrek aan duidelijkheid over de verwerking door HR2day belet instellingen om hun betrokkenen naar behoren te informeren over de verwerking van hun persoonsgegevens en over eventuele verdere verwerking die kan plaatsvinden.

De kans dat er sprake is van verlies van controle is waarschijnlijker wel dan niet, aangezien de huidige privacyverklaring de mogelijkheid openlaat dat HR2day klantgegevens verwerkt voor eigen doeleinden. De verdere verwerking veroorzaakt ernstige impact, aangezien het onduidelijk is om welke persoonsgegevens het gaat en de gegevens gevoelig of bijzonder kunnen zijn. Een doel als “Het creëren van interesseprofielen voor het promoten van relevante producten en diensten (profilering)” is ook niet in overeenstemming met de oorspronkelijke doeleinden van de instellingen en de redelijke verwachtingen van de betrokkenen. Dit vormt daarom een hoog risico.

16.7 Verlies van controle over gegevens over gebruikerstevredenheid

HR2day verzamelt via pop-ups gegevens over de gebruikerstevredenheid met het oog op dienstverbetering. Instellingen kunnen deze functionaliteit niet uitschakelen, hebben geen toegang tot deze gegevens en kunnen geen invloed uitoefenen op wat HR2day verzamelt. Deze beoordelingen maken geen deel uit van de verwerkersovereenkomsten met de instellingen en instellingen hebben geen mogelijkheid om HR2day instructies te geven over deze verwerking. De verwerking door HR2day van gegevens over de gebruikerstevredenheid ten behoeve van dienstverbetering leidt tot een onverenigbare verdere verwerking van persoonsgegevens voor HR2day’s eigen dienstverbeteringsdoeleinden.

De kans dat dit gebeurt is waarschijnlijker wel dan niet, aangezien het de huidige praktijk van HR2day is om dit te doen. Er is enige impact op de betrokkenen, aangezien het feit dat zij geen reden hebben om te verwachten dat HR2day hun gegevens zal verwerken voor eigen dienstverbetering, een verlies van controle veroorzaakt. De betreffende dataset is echter beperkt. Daarom is dit een hoog risico.

16.8 Verlies van controle en vertrouwelijkheid door ongeoorloofde toegang in derde landen

Tijdens het technisch onderzoek zijn overdrachten buiten de EER vastgesteld met betrekking tot subverwerker SignRequest voor het elektronisch ondertekenen van

overeenkomsten, subverwerker Expo voor het verzenden van meldingen via de mobiele app en Google voor het gebruik van de Google Maps-integratie. De overgedragen gegevens kunnen klantgegevens zijn, maar ook andere gegevens zoals loggegevens. De overdrachten vonden deels plaats naar de VS, waar het Data Privacy Framework van toepassing is, maar het is onduidelijk of er nog meer (verdere) overdrachten hebben plaatsgevonden.

Aangezien deze doorgiften niet wettelijk zijn beschermd in de verwerkersovereenkomsten en er geen andere maatregelen zijn om de betreffende persoonsgegevens te beschermen, is de kans op verlies van controle waarschijnlijker wel dan niet. Dit geldt met name voor SignRequest, dat heeft aangetoond dat het instellingen niet in staat kan stellen gegevens te verwerken op een manier die in overeenstemming is met de AVG. De gevolgen voor de rechten en vrijheden van betrokkenen kunnen, indien dit gebeurt, ernstige impact zijn, afhankelijk van het soort persoonsgegevens dat wordt bekendgemaakt en de partij waaraan deze worden bekendgemaakt. Dit is daarom een hoog risico

16.9 Verlies van controle over subverwerkers en ontvangers door ontbrekende of onjuiste overeenkomsten

HR2day heeft een verwerkersovereenkomst met Expo, maar heeft de bijbehorende dienstovereenkomst niet aan SURF verstrekt. Er is een dienstovereenkomst en een subverwerkersovereenkomst met SignRequest, maar SignRequest eist ook dat gebruikers akkoord gaan met hun eigen privacyverklaring wanneer HR2day-gebruikers worden doorgestuurd naar hun diensten. Dit zorgt voor een tegenstrijdige boodschap over de rol van SignRequest. Bovendien zijn er enkele ontvangers waarmee geen enkele overeenkomst is gesloten. Deze ontvangers zijn Google en Apple, die gegevens over betrokkenen verwerken bij het gebruik van de HR2day-app en bij het gebruik van de Google Maps-integratie. Zij zouden ofwel subverwerkers moeten zijn, wat betekent dat HR2day subverwerkersovereenkomsten met hen zou moeten hebben, ofwel derde ontvangers die gezamenlijke/onafhankelijke verwerkingsverantwoordelijken zijn. In het laatste geval moeten instellingen toestemming geven voor het verstrekken van hun persoonsgegevens aan deze partijen.

Het ontbreken van documentatie leidt tot een gebrek aan transparantie over de gegevens die door deze partijen worden verwerkt en tot een verlies van controle over deze gegevens. De kans dat dit gebeurt is waarschijnlijker wel dan niet, aangezien de documentatie momenteel ontbreekt. Dit kan ernstige impact toebrengen aan betrokkenen, aangezien het ontbreken van overeenkomsten betekent dat er helemaal geen controle is over deze gegevens en betrokkenen niet in staat zijn hun rechten als betrokkene uit te oefenen. Daarom is dit een hoog risico.

16.10 Verlies van vertrouwelijkheid door het ontbreken van 'read access logging'

Het ontbreken van registratie van gegevenstoegang (read access logging) vergroot het risico dat bij een autorisatiefout of incident niet kan worden vastgesteld of onbevoegden persoonsgegevens hebben ingezien. Daardoor is het bij een mogelijk datalek onmogelijk vast te stellen of, en wiens, persoonsgegevens door onbevoegden zijn ingezien. Dit betekent dat instellingen geen adequate en gerichte maatregelen kunnen nemen.

Er bestaat een redelijke kans dat deze gevolgen zich voordoen, omdat het ontbreken van logboekregistratie van leestoegang het moeilijk maakt om ongeoorloofde inzage te controleren en te beperken. Dit leidt tot ernstige impact, omdat er mogelijk sprake is van bijzondere en/of gevoelige persoonsgegevens en omdat er toegang kan plaatsvinden door partijen zowel binnen als buiten de organisatie. Dit is een hoog risico.

16.11 Schending van het beginsel van minimale gegevensverwerking door het opnemen van te brede lijsten met redenen voor verzuim

Te brede lijsten met redenen voor verzuim in HR2day vormen een inbreuk op het AVG-beginsel van minimale gegevensverwerking. Dit beginsel schrijft voor dat verzamelde persoonsgegevens toereikend en relevant moeten zijn en beperkt moeten blijven tot wat nodig is voor de specifieke doeleinden waarvoor ze worden verwerkt. De mogelijkheid voor instellingen om hun eigen categorieën voor ziekte of andere redenen voor verzuim te definiëren, leidt tot risico's van buitensporige en onnodige verzameling van gevoelige gegevens. Dit kan leiden tot de verwerking van gezondheidsgegevens en andere bijzondere categorieën gegevens die verder gaan dan het noodzakelijke minimum, waardoor de privacy van werknemers wordt geschonden en de kans op oneigenlijk gebruik van gegevens of inbreuken toeneemt.

De kans dat dit risico zich voordoet, hangt sterk af van de ervaring van het team van de instellingen dat HR2day configureert en beheert, dus het is waarschijnlijker dat het zich voordoet dan niet. De impact kan ernstige impact zijn vanwege de aard van de doeleinden die HR2day bij instellingen vervult. Daarom is dit een hoog risico.

16.12 Verlies van controle door open tekstvelden

De aanwezigheid van mogelijk talrijke open tekstvelden in HR2day, hoewel deze vaak correct zijn gelabeld met de beoogde doeleinden, vormt een risico op verlies van controle over persoonsgegevens. Niet alle methoden voor veldvalidatie zijn geïmplementeerd, wat kan leiden tot inconsistente of onnauwkeurige gegevensinvoer. Instellingen/klanten kunnen ook nieuwe tekstvelden aanmaken zonder de juiste doeleinden of adequate labeling toe te voegen, waardoor het risico op ongecontroleerde gegevensverzameling en -verwerking wordt vergroot. Vanuit privacyoogpunt zijn open tekstvelden bijzonder gevoelig omdat gebruikers elk type persoonlijke of gevoelige informatie kunnen invoeren, waardoor de beoogde reikwijdte van de gegevensverwerking mogelijk wordt overschreden of de beginselen van minimale gegevensverwerking worden geschonden.

De kans dat dit gebeurt is waarschijnlijker wel dan niet, aangezien dit sterk afhankelijk is van de ervaring van het team van de instellingen dat HR2day configureert en beheert. De impact kan ernstig zijn , afhankelijk van het type gegevens dat wordt gedeeld, dat gevoelig of bijzonder kan zijn. Daarom is dit een hoog risico.

16.13 Gebrek aan juistheid door handmatige registratie van persoonsgegevens

De mogelijkheid om persoonsgegevens handmatig in HR2day te registreren en te bewerken, brengt het risico van onjuistheid met zich mee als gevolg van menselijke fouten. Managers en HR-medewerkers kunnen rechtstreeks persoonlijke gegevens invoeren en wijzigen, zoals arbeidsrelaties, salarissen, verlofgegevens en gebruikersinformatie. Het ontbreken van geautomatiseerde validatie of standaardcontroles tijdens handmatige gegevensinvoer

vergroot de kans dat onjuiste of verouderde informatie wordt vastgelegd. Dit kan leiden tot onbedoelde gevolgen, zoals het delen van informatie met onbevoegde partijen, financiële discrepanties en het ten onrechte weigeren van verlof aan werknemers. Deze situatie onderstreept het belang van het implementeren van corrigerende controles, zoals invoervalidatie, audittrails en periodieke gegevenscontroles, om de juistheid van de gegevens te verbeteren en privacyrisico's te verminderen. Uiteindelijk waarborgt het waarborgen van een hoge gegevenskwaliteit niet alleen de privacy van individuen, maar ook de integriteit en betrouwbaarheid van HR-activiteiten.

De kans dat deze onjuistheden zich voordoen, wordt als groter dan klein beschouwd, aangezien het risico afhankelijk is van de ervaring van het team van de instelling dat HR2day configureert en beheert, in combinatie met het ontbreken van huidige risicobeperkende maatregelen. Zonder in het systeem geïntegreerde mechanismen voor foutdetectie of -correctie kunnen fouten onopgemerkt blijven bestaan en zich verspreiden via gerelateerde processen. Aangezien deze fouten rechtstreeks van invloed zijn op de rechten en aanspraken van personen en tastbare en ingrijpende gevolgen hebben, kan de impact voor de betrokkenen ernstig zijn. Vanwege de ernstige impact en de redelijke waarschijnlijkheid is dit een hoog risico.

16.14 Verlies van controle over bewaartermijnen door gebrek aan automatisering

HR2day beschikt momenteel niet over geautomatiseerde functionaliteit om persoonsgegevens te verwijderen zodra bewaartermijnen verstrijken, en het kan geen waarschuwingen genereren wanneer dergelijke termijnen aflopen. Onderscheid tussen categorieën persoonsgegevens met verschillende bewaarvereisten is evenmin gesystematiseerd. De huidige aanpak is gebaseerd op periodieke handmatige verwerking van signaallijsten, die waarschijnlijk inconsistent worden beheerd met lange intervallen tussen verwijderingsacties. Dit creëert een aanzienlijk risico dat persoonsgegevens langer dan nodig worden bewaard, wat in strijd is met de beginselen van minimale gegevensverwerking en leidt tot een verlies van individuele controle en vertrouwelijkheid.

De kans dat dit risico zich voordoet, is waarschijnlijker wel dan niet, vanwege de afhankelijkheid van handmatige processen die kwetsbaar zijn voor menselijke fouten en onoplettendheid. Dit kan ernstige impact veroorzaken, aangezien dit probleem van invloed is op het beginsel van opslagbeperking voor alle persoonsgegevens die in HR2day worden beheerd, met inbegrip van bijzondere categorieën van gevoelige gegevens. Daarom is dit een hoog risico.

16.15 Verlies van vertrouwelijkheid als gevolg van de standaardinstelling voor verticale overerving van rechten

De standaardinstelling van verticale overerving van rechten binnen het systeem leidt tot een conflict met het door de AVG voorgeschreven beginsel van minimale gegevensverwerking. Verticale overerving maakt het mogelijk dat rechten automatisch door de organisatielagen worden doorgegeven, wat kan resulteren in bredere toegang tot persoonsgegevens dan nodig is. Hoewel het uitschakelen van deze overerving de privacybescherming zou verbeteren door de toegang te beperken tot alleen degenen die daartoe bevoegd zijn, creëert het in sommige gevallen ook operationele uitdagingen voor organisaties die HR-taken toewijzen aan managers ‘in de lijn’. Deze situatie brengt een aanzienlijk risico op

verlies van vertrouwelijkheid met zich mee, omdat over e geërfde inzagerechten gebruikers in staat kunnen stellen persoonsgegevens te bekijken of te beheren die buiten hun legitieme bevoegdheid vallen. Om in overeenstemming te zijn met het beginsel van minimale gegevensverwerking, moet het systeem gedetailleerde toegangscontrole mogelijk maken die het op passende wijze beperken van de toegang van groepen ondersteunt, terwijl de noodzakelijke functionele workflows behouden blijven.

De kans dat dit risico zich voordoet, is redelijk. Hoewel HR2day instellingen informeert over de mogelijkheid om deze functie uit te schakelen, is de instelling voor verticale overerving van rechten standaard ingeschakeld. Instellingen die HR-taken toewijzen aan managers in de lijn moeten verticale overerving van rechten inschakelen zodat zij hun taken kunnen uitvoeren, en realiseren zich mogelijk niet de impact hiervan, waardoor zij niet de juiste maatregelen nemen om schade aan betrokkenen te voorkomen. De impact is ernstig, omdat buitensporige overgenomen inzagerechten gebruikers in staat kunnen stellen om persoonsgegevens, waaronder gevoelige en bijzondere categorieën van persoonsgegevens, te bekijken of te beheren buiten hun legitieme werkterrein. Daarom is dit een hoog risico.

16.16 Verlies van controle door gebrek aan beheer van encryptiessleutels

Salesforce is als subverwerker verantwoordelijk voor hosting, encryptie en back-ups, en beheert bovendien de encryptiessleutels die bij deze processen worden gebruikt. Hoewel de subverwerker technische en organisatorische maatregelen moet nemen om de beveiliging te waarborgen, blijft de uiteindelijke verantwoordelijkheid voor de naleving van de gegevensbeschermingsvoorschriften bij de verwerkingsverantwoordelijke liggen. Het feit dat HR2day het sleutelbeheer aan een subverwerker heeft gedelegeerd, voegt een extra risico toe: tekortkomingen in het sleutelbeheer kunnen leiden tot ongeoorloofde ontsleuteling en datalekken. Aangezien HR2day zelf niet verantwoordelijk is voor het sleutelbeheer of de opslag van de sleutels, moet de verwerkingsverantwoordelijke er via contractuele en auditmechanismen voor zorgen dat de subverwerker robuuste praktijken voor het beheer van encryptiessleutels hanteert, waaronder veilige sleutelopslag, toegangsbeperkingen, rotatiebeleid en incidentmonitoring. Zonder strikte controles en transparantie kan het vertrouwen op een subverwerker voor sleutelbeheer de beveiligingspositie verzwakken en de melding van inbreuken bemoeilijken als sleutels gecompromitteerd raken. Door HR2day de encryptiessleutels te laten opslaan en beheren, wordt ook gewaarborgd dat er geen persoonsgegevens door Salesforce kunnen worden gedeeld indien zij openbaarmakingsbevelen ontvangen van buitenlandse autoriteiten.

Om aan te tonen hoe de gegevens in de HR2day-applicatie worden versleuteld, verwees HR2day naar algemene Salesforce-beveiligingscertificeringen en andere Salesforce-documentatie. Deze documentatie beschrijft, verspreid over ten minste vier verschillende documenten[1] , de soorten encryptie die Salesforce aanbiedt en biedt de garantie dat klantgegevens en back-ups in rust worden versleuteld. Ze bieden echter geen gedetailleerd inzicht in hoe encryptie in het algemeen wordt geïmplementeerd voor Salesforce-diensten (encryptiesprotocollen, hoe vaak sleutels worden gewisseld, waar sleutels worden opgeslagen, enz.), en zeker niet specifiek voor HR2day. De enige bekende feiten zijn dat HR2day databaseencryptie gebruikt en geen gebruik maakt van Salesforce Shield. HR2day

[1] C5-rapport voor Salesforce-services op Hyperforce; Beveiliging, privacy en architectuur van Hyperforce; Systeem- en organisatie (SOC2) Type 2 voor Salesforce Services op Hyperforce; Overzicht van opslagencryptie door Salesforce Services zelf.

bevat gevoelige en bijzondere categorieën gegevens, die versterkte beschermingsmaatregelen vereisen die verder gaan dan standaard waarborgen, omdat openbaarmaking ervan tot aanzienlijke schade kan leiden. Salesforce raadt zelf aan om voor gevoelige gegevens het gebruik van aanvullende Platform Encryption (die encryptie op celniveau biedt) te overwegen. Versleuteling op celniveau biedt een extra beschermingslaag voor het geval de hoofdencryptiessleutels gecompromitteerd raken.

De kans dat er controleverlies optreedt zodra er een inbreuk op de beveiliging plaatsvindt, is waarschijnlijker wel dan niet, aangezien HR2day volledig afhankelijk is van Salesforce voor het beheer van de encryptiesmethoden. De impact is ernstig, aangezien dit probleem gevolgen heeft voor alle persoonsgegevens die in HR2day worden beheerd, inclusief speciale categorieën van gevoelige gegevens, waarvoor standaard geen aanvullende maatregelen zijn getroffen. Daarom is dit een hoog risico.

Risico's als gevolg van het aanbieden van een mobiele app via de app-winkels van Google en Apple

Op het moment van publicatie heeft SURF nog geen conclusie getrokken over de impact van de volgende twee risico's, die verband houden met de verwerking door Google en Apple bij het gebruik van mobiele apps. De overwegingen en maatregelen die SURF heeft geïdentificeerd, staan hieronder beschreven. SURF doet echter nader onderzoek naar de impact van deze risico's en het effect van beschikbare maatregelen op de risico's. Hierover volgt later een publicatie. In de tussentijd kunnen instellingen op basis van hun eigen beoordelingen actie ondernemen.

16.17 Verlies van controle over verwerkte persoonsgegevens door installatie van mobiele app via app-winkel van derden

Het risico dat gepaard gaat met het aanbieden van de HR2day-mobiele app via de Apple App Store en Google Play Store ligt in de automatische koppeling die tot stand komt tussen het app-gebruik en het persoonlijke Apple- of Google-account van de gebruiker. Deze koppeling stelt deze platformaanbieders in staat om inzicht te krijgen in de installatie van de app, wat kan leiden tot indirecte identificatie van de relatie met HR2day. Omdat deze verwerking niet strikt noodzakelijk is voor de werking van de app, is dit in strijd met het Privacy by Default-principe en leidt dit tot verlies van controle over persoonsgegevens.

De kans dat dit risico zich voordoet, is waarschijnlijker wel dan niet, aangezien er een verlies van controle optreedt zodra de app via een app-store wordt gedownload. Bijgevolg vloeien persoonsgegevens over werknemers onvermijdelijk naar derden zoals Apple en Google, wat de vertrouwelijkheid in gevaar kan brengen en het risico voor de rechten en vrijheden van werknemers vergroot. Dit leidt tot de potentiële blootstelling van persoonsgegevens zonder expliciete noodzaak en de betrokkenheid van grote platformaanbieders.

Er moeten alternatieven met minder inbreuken op de privacy worden overwogen om de gegevens van gebruikers beter te beschermen en naleving van de vereisten inzake minimale gegevensverwerking te waarborgen.

16.18 Verlies van controle door de verwerking van pushmeldingen door Google en Apple

Dit is een risico dat in het algemeen geldt voor alle applicaties die gebruikmaken van de push-infrastructuur van Google of Apple.

De mobiele HR2day-app verstuurt pushmeldingen. De pushmeldingen leiden zowel tot de overdracht van metadata en inhoud naar Google en Apple. De metadata betreft gegevens zoals apparaat-ID's, IP-adressen en mogelijk het Google- of Apple-account van de student. De inhoud betreft de berichten, indien die inhoud onversleuteld wordt verzonden, wat noodzakelijkerwijs het geval is bij het onderdeel “meldingsberichten” van de pushmeldingen. De inhoud van deze berichten is zichtbaar voor en wordt verwerkt door Google en Apple. Aangezien het niet noodzakelijk is om persoonsgegevens in meldingen op te nemen, vormt dit een inbreuk op het subsidiariteitsbeginsel. Onderwijsinstellingen bepalen zelf de inhoud van de berichten en kunnen privacyvriendelijke keuzes maken door geen persoonsgegevens op te nemen.

Ongeacht de inhoud van de berichten betekent het gebruik van meldingen dat de inhoud ervan systematisch door Google wordt verwerkt. Het is mogelijk deze verwerking te beperken door gebruik te maken van een versleutelde datapayload, hetzij bovenop het meldingsbericht, hetzij afzonderlijk. Als een student beschikt over Unified Push, een alternatieve push-infrastructuur voor Android, kan de app hier ook gebruik van maken en terugvallen op Google indien dit niet beschikbaar is. Aangezien beide beperkende maatregelen ontbreken, voldoet het gebruik van meldingen niet
niet aan de subsidiariteitsvereiste.

De kans dat er sprake is van een verlies van controle is waarschijnlijker wel dan niet, aangezien meldingen een standaardonderdeel zijn van de HR2day-app en het verlies van controle optreedt zodra Google of Apple de melding ontvangt.

Deel D Beschrijving van de voorgestelde maatregelen

Driving innovation together

17 Maatregelen

In dit hoofdstuk worden de technische, organisatorische en juridische maatregelen beschreven die instellingen en HR2day kunnen nemen om de hierboven beschreven risico's te beperken. Voor elk risico beschrijft de bovenste helft van de tabel het huidige risico en toont deze de risicoscore uit deel C. De onderste helft van de tabel beschrijft de maatregelen die HR2day en de instellingen kunnen nemen en geeft een score voor het restrisico.

Deze referentie-DPIA gaat uit van een adequate basis van organisatorische privacyvolwassenheid. De toepasbaarheid en prioritering van zowel risico's als maatregelen zullen echter aanzienlijk variëren, afhankelijk van de huidige proces-, technische en governancevolwassenheid van elke instelling. Wij raden elke instelling die twijfelt aan haar gereedheid ten zeerste aan om een zelfevaluatie uit te voeren aan de hand van de gepresenteerde risico's en maatregelen of om advies in te winnen bij collega-instellingen, SURF en/of MBO Digitaal. Het is van het grootste belang dat elke instelling dit overzicht kritisch toetst aan haar eigen operationele context en technische infrastructuur.

Salesforce-risico's

Verlies van controle en vertrouwelijkheid door toegang tot persoonsgegevens door buitenlandse autoriteiten						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
0	Toegang tot persoonsgegevens door buitenlandse autoriteiten	Verlies van controle en vertrouwelijkheid	**Waarschijnlijker weldan niet**	**Ernstig**	**Hoog**	
	Maatregelen Instelling	**Leverancier van maatregelen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Restrisico**
	-*	Neem alle rechtmatige overdrachten in verwerkersovereenkomst tussen instellingen en HR2day op.	**Heel klein**	**Ernstig**	**Laag**	

*Hoewel er juridisch gezien geen aanvullende maatregelen aan de kant van de instelling nodig zijn zolang het Data Privacy Framework bestaat, is het raadzaam om de geopolitieke situatie periodiek te beoordelen – met name met betrekking tot de waarschijnlijkheid dat risico's zich voordoen – om te zien of aanpassing van de risicobeoordeling noodzakelijk is.

Verlies van controle door een gebrek aan transparantie over de verwerking van gebruiksgegevens voor doeleinden van Salesforce						
Referentie	**Oorzaak**	**Gevolg**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	

	Gebrek aan transparantie over verdere verwerking voor doeleinden van Salesforce	Verlies van controle	**Waarschijnlijker wel dan niet**	**Ernstig**	**Hoog**	**Huidig risico**
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
0	Update de verwerkersovereenkomst tussen HR2day en instellingen met: alle categorieën persoons gegevens, inclusief gebruiksgegevens indien van toepassing, die HR2day en subverwerkers namens instellingen verwerken; legitieme zakelijke doeleinden waarvoor HR2day en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor HR2day en subverwerkers geen persoonsgegevens mogen verwerken; auditrecht voor instellingen met betrekking tot de verwerkersovereenkomst.	Update verwerkersovereenkomst tussen HR2day en instellingen met: alle categorieën persoonsgegevens, inclusief gebruiks gegevens indien van toepassing, die HR2day en subverwerkers namens instellingen verwerken; legitieme zakelijke doeleinden waarvoor HR2day en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor HR2day en subverwerkers geen persoonsgegevens mogen verwerken; auditrecht voor instellingen met betrekking tot de verwerkersovereenkomst.	**Heel klein**	**Ernstig**	**Laag**	**Restrisico**
	Afzien van het verstrekken van trainingsgegevens aan de globale modellen bij het gebruik van Einstein Search.	Update verwerkersovereenkomst tussen HR2day en Salesforce met: alle categorieën persoonsgegevens, inclusief gebruiksgegevens indien van toepassing, die Salesforce namens instellingen verwerkt; legitieme zakelijke doeleinden waarvoor en onder welke voorwaarden Salesforce persoonsgegevens mag verwerken; doeleinden waarvoor Salesforce geen persoonsgegevens mag verwerken; auditrecht voor instellingen met betrekking tot de verwerkersovereenkomst.				

Onvermogen om de inzagerechten van de betrokkene tot persoonsgegevens uit te oefenen						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	

0	Onvolledig antwoord op verzoek om inzage van de betrokkene.	Onvermogen om het recht op inzage in persoonsgegevens uit te oefenen	**Waarschijnlijker wel dan niet**	**Ernstig**	**Hoog**	**Huidig risico**
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Restrisico**
		Verbeter het DSAR-beleid zodat HR2day volledige toegang kan bieden tot alle persoonsgegevens die zij en hun subverwerkers verwerken.	**Heel klein**	**Ernstig**	**Laag**	

Verlies van controle door een gebrek aan transparantie over de verwerking van persoonsgegevens via cookies						
Referentie	**Oorzaak**	**Gevolg**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
0	Onvolledige cookieverklaring/documentatie.	Betrokkenen kunnen zich niet informeren over de verwerking van persoonsgegevens via cookies.	**Waarschijnlijker wel dan niet**	**Ernstig**	**Hoog**	
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Restrisico**
		Alle gebruikers van HR2day voorzien van een volledige cookieverklaring.	**Heel klein**	**Ernstig**	**Laag**	

Verlies van controle doordat men zich moet registreren voor updates van subverwerkers Salesforce						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
0	Verplichte registratie voor updates van subverwerkers bij Salesforce.	Verlies van controle.	**Redelijk**	**Ernstig**	**Hoog**	
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Restrisico**
		Implementeer een proces waarbij HR2day de subverwerkers van Salesforce aan instellingen doorgeeft.	**Heel klein**	**Ernstig**	**Laag**	

Algemene risico's

Verlies van controle door een gebrek aan transparantie over de verwerking van persoonsgegevens voor doeleinden van HR2day						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
0	Gebrek aan transparantie over verdere verwerking voor doeleinden van HR2day	Verlies van controle	**Waarschijnlijker wel dan niet**	**Ernstig**	Hoog	**Huidig risico**
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
	Update de verwerkersovereenkomst tussen HR2day en instellingen met: alle categorieën persoonsgegevens, inclusief gebruiksgegevens indien van toepassing, die HR2day en subverwerkers namens instellingen verwerken; legitieme zakelijke doeleinden waarvoor HR2day en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor HR2day en subverwerkers geen persoonsgegevens mogen verwerken; auditrecht voor instellingen met betrekking tot de verwerkersovereenkomst.	Update verwerkersovereenkomst tussen HR2day en instellingen met: alle categorieën persoonsgegevens, inclusief gebruiksgegevens indien van toepassing, die HR2day en subverwerkers namens instellingen verwerken; legitieme zakelijke doeleinden waarvoor HR2day en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor HR2day en subverwerkers geen persoonsgegevens mogen verwerken; auditrecht voor instellingen met betrekking tot de verwerkersovereenkomst.	**Heel klein**	**Ernstig**	Laag	**Restrisico**
		Update privacyverklaring HR2day.				

Verlies van controle over gegevens over gebruikerstevredenheid						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
0	Verzameling van tevredenheidsgegevens met HR2day als verwerkingsverantwoordelijke voor verdere verwerking.	Verlies van controle.	**Waarschijnlijker wel dan niet**	**Ernstig**	Hoog	**Huidig risico**
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
		Neem deze verwerking op in de verwerkersovereenkomst met HR2day als verwerker en geef instellingen zinvolle controle (door middel van transparantie) en keuzes bij deze verwerking.	**Heel klein**	**Ernstig**	Laag	**Restrisico**

Verlies van controle en vertrouwelijkheid door ongeoorloofde toegang in derde landen						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
0	Ongeautoriseerde toegang door partijen in derde landen.	Verlies van controle en vertrouwelijkheid.	**Waarschijnlijker wel dan niet**	**Ernstig**	Hoog	
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
	Stop met het gebruik van SignRequest.	Identificeer alle overdrachten, in ieder geval naar Expo en Google.	**Heel klein**	**Ernstig**	Laag	**Restrisico**
		Neem rechtmatige doorgiften aan subverwerkers op in de verwerkersovereenkomst tussen HR2day en de instelling.				
		Informeer instellingen over de partijen waaraan persoonsgegevens worden doorgegeven en waarmee zij rechtstreeks overeenkomsten moeten sluiten.				
		Zorg ervoor dat klanten die stoppen met het gebruik van SignRequest een kopie kunnen krijgen van de verwerkte gegevens van hun betrokkenen en deze indien nodig kunnen verwijderen.				

Verlies van controle over subverwerkers en ontvangers door ontbrekende of onjuiste overeenkomsten						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
0	Geen of onjuiste afspraken tussen HR2day en haar subverwerkers.	Verlies van controle.	**Waarschijnlijker wel dan niet**	**Ernstig**	Hoog	
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
		Beoordeel of Google en Apple in aanmerking komen als subverwerkers, gezamenlijke verwerkingsverantwoordelijken of externe ontvangers.	**Heel klein**	**Ernstig**	Laag	**Restrisico**
		Neem Google en Apple op in de verwerkersovereenkomst tussen HR2day en instellingen.				

		Sluit de benodigde overeenkomsten met Google en Apple.				

Verlies van vertrouwelijkheid door het ontbreken van 'read access logging'						
Referentie	**Oorzaak**	**Gevolg**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
0Fout! V erwijzingsbron niet gevonden.	Ontbreken van 'read access logging'	Verlies van vertrouwelijkheid.	**Waarschijnlijker wel dan niet**	**Ernstig**	Hoog	
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Restrisico**
	Implementeer ten minste 'logboekregistratie van leestoegang' voor categorieën gevoelige en bijzondere gegevens.	Schakel 'read access logging' in voor categorieën van gevoelige en bijzondere gegevens en minimaal voor de proxy-inlogfunctionaliteit.	**Heel klein**	**Ernstig**	Laag	
	Implementeer logboekregistratie van leestoegang voor activiteiten die beheerders uitvoeren met behulp van de proxy-aanmelding.					
	Informeer gebruikers zonder onnodige vertraging dat er iemand zich voor hen heeft uitgegeven.					

Schending van het beginsel van minimale gegevensverwerking door het opnemen van te brede lijsten met redenen voor afwezigheid						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
0	Te brede (selectie)lijsten voor redenen van afwezigheid.	Schending van het beginsel van minimale gegevensverwerking.	**Waarschijnlijker wel dan niet**	**Ernstig**	Hoog	
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Restrisico**
	Gebruik alleen keuzelijsten om informatie te verzamelen over de reden van de afwezigheid van medewerkers en een vaste set velden om aanvullende informatie over hun afwezigheid te verzamelen.	Geef instellingen instructies over het gebruik van keuzelijsten voor het verzamelen van gevoelige en bijzondere categorieën gegevens.	**Heel klein**	**Ernstig**	Laag	
	Laat de keuzelijst voor verzuim en de vaste set velden beoordelen door de privacyafdeling, om ervoor te zorgen dat ze in overeenstemming zijn met					

	de AVG-vereisten en de beschikbare richtlijnen.					
	Zorg ervoor dat gebruikers van HR2day goed worden geïnstrueerd en getraind over welke soorten gegevens over de afwezigheid van werknemers mogen worden verwerkt.					

Verlies van controle door open tekstvelden						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
	Open tekstvelden.	Verlies van controle.	**Waarschijnlijker wel dan niet**	**Ernstig**	**Hoog**	
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
0	Gebruik open tekstvelden alleen met een duidelijk doel.	Geef instellingen instructies over hoe ze open tekstvelden kunnen gebruiken op een manier die de beginselen van minimale gegevensverwerking respecteert.	**Heel klein**	**Ernstig**	**Laag**	**Restrisico**
	Formuleer vragen op een manier die duidelijk maakt welke (gevoelige/bijzondere) persoonsgegevens wel en niet in een open tekstveld moeten worden ingevuld en maak gebruik van de beschikbare informatiepictogrammen.	Bied voldoende opties voor veldvalidatie om onjuiste gegevensverwerking te voorkomen.				
	Zorg ervoor dat gebruikers van HR2day goed worden geïnstrueerd en getraind over welke soorten gegevens in open tekstvelden mogen worden verwerkt.					

Gebrek aan juistheid door handmatige registratie van persoonsgegevens						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
0	Handmatige registratie van persoonsgegevens.	Gebrek aan juistheid.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	

	Maatregelen instelling	Maatregelen leverancier	Waarschijnlijkheid	Impact	Risicoscore	
	Automatiseer de gegevensinvoer waar mogelijk, bijvoorbeeld door HR2day te koppelen aan het wervingssysteem.	Bied voldoende opties voor veldvalidatie om onjuiste gegevensverwerking te voorkomen.	**Heel klein**	**Ernstig**	**Laag**	**Restrisico**
	Zorg ervoor dat HR-medewerkers goed zijn geïnstrueerd en getraind in de procedures van de instellingen voor het zorgvuldig registreren van persoonsgegevens.					

Verlies van controle over bewaartermijnen door gebrek aan automatisering						
Referentie	**Oorzaak**	**Gevolg**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
0	Geen automatisering bij het handhaven van bewaartermijnen	Verlies van controle	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
	Bepaal en beheer bewaartermijnen voor persoonsgegevens in HR2day.	Geef informatie en instructies over de procedure voor het verwijderen van gegevens met behulp van signaallijsten aan instellingen.	**Heel klein**	**Ernstig**	**Laag**	**Restrisico**
	Zorg ervoor dat de bewaartermijnen worden nageleefd door processen in te voeren om deze af te dwingen, bijvoorbeeld door gebruik te maken van de geautomatiseerde bewaartermijnen voor documenten.	Instellingen faciliteren bij het handhaven van hun bewaartermijnen door de mogelijkheden voor technische configuratie en beheer van bewaartermijnen per groep persoonsgegevens in HR2day te verbeteren.				

Verlies van vertrouwelijkheid door de standaardinstelling voor verticale overerving van rechten						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
0	Verticale overerving van inzagerechten is standaard ingeschakeld.	Verlies van vertrouwelijkheid.	**Redelijk**	**Ernstig**	**Hoog**	
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Restrisico**

	Schakel de verticale overerving van rechten uit, tenzij het nodig is om deze instelling te gebruiken.	Informeer instellingen proactief over de privacygevolgen van de instelling voor verticale overerving van rechten en bied hen de keuze om deze in of uit te schakelen.	**Heel klein**	**Ernstig**	**Laag**	
	Beperk de toegang tot persoonsgegevens voor functies die deze gegevens niet nodig hebben om hun taken uit te voeren.	Werk samen met instellingen om de mogelijkheden te verbeteren om het beginsel van minimale gegevensverwerking na te leven terwijl de instelling voor verticale overerving van rechten is ingeschakeld, waardoor de administratieve lasten worden verminderd, OF stel hen in staat de noodzakelijke workflows uit te voeren terwijl de instelling is uitgeschakeld.				
	Wees transparant tegenover betrokkenen over het gebruik van de instelling voor verticale overerving van rechten en over wie toegang heeft tot hun gegevens.					

Verlies van controle door gebrek aan beheer van encryptiesleutels						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	**Huidig risico**
	Verwerking van gevoelige en bijzondere categorieën gegevens.	Verlies van vertrouwelijkheid.	**Waarschijnlijker dan niet**	**Ernstig**	**Hoog**	
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
0	Beoordeel of encryptie op celniveau, encryptie met door de klant beheerde sleutels en eventuele andere aanvullende maatregelen nodig zijn voor speciale en gevoelige categorieën gegevens, rekening houdend met de specifieke gegevens die door de instelling worden verwerkt en de andere beveiligingsmaatregelen die van kracht zijn.	Informeer instellingen over de encryptiemethoden die worden gebruikt voor de HR2day-applicatie en het platform en over de mogelijkheid van aanvullende beveiligingsmaatregelen, zoals encryptie op celniveau en door HR2day beheerde encryptiessleutels.	**Heel klein**	**Ernstig**	**Laag**	**Restrisico**
		Werk samen met instellingen bij het beoordelen van het vereiste encryptiesniveau voor de persoonsgegevens in HR2day, met name voor de gevoelige en bijzondere categorieën persoonsgegevens.				

		Waar instellingen dit nodig achten, moeten aanvullende beveiligingsmaatregelen worden geïmplementeerd, zoals encryptie op celniveau en encryptiessleutels die door HR2day worden beheerd.				

Risico's van mobiele apps

Verlies van controle over de verwerkte persoonsgegevens door de installatie van de mobiele app via een app-store van een derde partij						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
0	Verlies van controle	Verlies van controle	**Waarschijnlijker dan niet**	**Nader te bepalen**	**Nader te bepalen**	**Huidig risico**
	Maatregelen instelling	**Leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
	Maak de app beschikbaar via sideloading.	De app beschikbaar stellen via sideloading.	**Nader te bepalen**	**Nader te bepalen**	**Nader te bepalen**	**Restrisico**
	Voer evenredigheids- en subsidiariteitsbeoordelingen uit met betrekking tot het aanbieden van de mobiele app via app-winkels en 'side-loading' en implementeer de resultaten.	Maak toegang via de mobiele browser vanaf mobiele apparaten mogelijk.				

Verlies van controle door de verwerking van pushmeldingen door Google en Apple						
Referentie	**Oorzaak**	**Gevolgen**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
0	Verplichte verzending van pushmeldingen via Google en Apple.	Verlies van controle	**Waarschijnlijker dan niet**	**Nader te bepalen**	**Nader te bepalen**	**Huidig risico**
	Maatregelen instelling	**Maatregelen leverancier**	**Waarschijnlijkheid**	**Impact**	**Risicoscore**	
	Neem geen persoonsgegevens op in de berichten die via pushmeldingen worden verzonden.	Optioneel: Implementeer Unified Push voor Android-gebruikers.	**Nader te bepalen**	**Nader te bepalen**	**Nader te bepalen**	**Rest risico**
	Voer evenredigheids- en subsidiariteitsbeoordelingen uit met betrekking tot het verzenden van pushmeldingen via Google en Apple of Unified Push en implementeer de resultaten.					

18 Conclusie

Deze DPIA heeft zestien hoge risico's voor betrokkenen geïdentificeerd en twee risico's waarvan het risiconiveau nog moet worden bepaald. Vijf van de hoge risico's houden verband met het gebruik van Salesforce als aanbieder van het platform waarop HR2day draait. Elf van de hoge risico's zijn algemene risico's, veroorzaakt door de manier waarop instellingen HR2day (waarschijnlijk) gebruiken of door het ontwerp van HR2day. Twee van de risico's houden verband met het gebruik van de mobiele app. Deze twee risico's bestaan voor elke app die gebruikmaakt van de app store en pushmeldingen.

Door deze maatregelen te implementeren worden alle hoge risico's gemitigeerd, waardoor alleen lage restrisico's overblijven. Hoewel het niet strikt noodzakelijk is om lage risico's te mitigeren, wordt dit wel aanbevolen.

Voor al deze risico's is er een tijdschema voor de implementatie van de maatregelen. Daarom kunnen instellingen HR2day blijven gebruiken. Als de hoge risico's worden beperkt, is voorafgaand overleg met de gegevensbeschermingsautoriteit niet vereist. SURF zal in 2027 een update over deze DPIA publiceren met een conclusie over de implementatie van de resterende maatregelen.