# DPIA HR2day

Applicatie voor personeels- en salarisadministratie

***Nederlandse vertaling (SIVON)***


| | |
|---|---|
| Auteur(s): | Sophia Gelpke & Jan Landsaat |
| Versie: | 1.0 |
| Datum: | 12 mei 2026 |
| Licentie: | Creative Commons Naamsvermelding 4.0 Internationaal |
| Nederlandse vertaling: | Dimitri Wouters en Job Vos (SIVON), versie 1.0 (16 juni 2026) |


**LET OP:** dit betreft de Nederlandse vertaling van de DPIA HR2day van SURF. De tekst van de originele Engelstalige versie is altijd leidend.

*Hoewel aan de totstandkoming van deze vertaling de uiterste zorg is besteed, aanvaarden SIVON en de oorspronkelijke auteur(s) geen aansprakelijkheid voor eventuele fouten, onvolkomenheden of schade als gevolg van het gebruik van dit document. Consulteer bij twijfel een in privacy gespecialiseerde specialist, jurist of advocaat voor advies over de toepassing van de DPIA voor uw eigen organisatie.*

# Inhoudsopgave

## Versiegeschiedenis

| Versie | Datum | Samenvatting van wijzigingen |
|---|---|---|
| 0.2 | 20 mei 2025 | Eerste concept van deel A, gedeeld met HR2day |
| 0.3 | 24 mei 2025 | Opmerkingen HR2day (Henk/Marco) verwerkt |
| 0.5 | 17 oktober 2025 | Volledig bijgewerkt deel A na review HR2day en interne review en toevoeging van delen B & C |
| 0.66 | 3 februari 2026 | Volledig concept-DPIA met HR2day-review op versie 0.5 verwerkt |
| 0.7 | 3 april 2026 | Volledige DPIA-versie met samenvatting, conclusie en HR2day-review op versie 0.66 verwerkt |
| 1.0 | 30 april 2026 | Definitieve DPIA-versie met bijgewerkte versiegeschiedenis, statustabel en oplegger |

# Voorwoord SIVON bij de Nederlandse vertaling

**SIVON stelt deze Nederlandse vertaling van de referentie-DPIA op HR2day beschikbaar voor schoolbesturen in het funderend onderwijs. De DPIA is door SURF uitgevoerd voor mbo-instellingen, hogescholen, universiteiten en de onderzoeksector. Met toestemming van SURF is de DPIA door SIVON vertaald, zodat ook schoolbesturen in het funderend onderwijs de uitkomsten eenvoudig kunnen gebruiken bij hun eigen beoordeling van HR2day.**

De vertaling van wat SURF referentie-DPIA noemt, is wat SIVON de centrale DPIA noemt. Bij deze vertaling hoort de door SIVON ontwikkelde ***lokale DPIA HR2day*** als aparte bijlage om de DPIA op HR2day organisatie-specifiek te maken. Deze centrale DPIA is geen vervanging voor de zelf uit te voeren DPIA: rekening houdend met het specifieke gebruik van HR2day, gegevenscategorieën, autorisatiemodel en risico's moet elk schoolbestuur zelf een DPIA uitvoeren.

De keuze voor een Nederlandse vertaling is gemaakt omdat de toepassing van de DPIA in de praktijk vaak plaatsvindt in het funderend onderwijs waar Nederlands de voertaal is. Het oorspronkelijke rapport is opgesteld in het Engels en bevat juridische, technische en contractuele bevindingen. Deze Nederlandstalige versie verlaagt de drempel om de risico's, maatregelen en verantwoordelijkheden te begrijpen en toe te passen. SURF spreekt over (onderwijs- en onderzoeks)instellingen, in de vertaling is deze terminologie aangehouden waarbij met de term instellingen ook schoolbesturen in het funderend onderwijs worden bedoeld.

Deze vertaling is nadrukkelijk bedoeld als hulpmiddel. De originele Engelstalige DPIA van SURF is en blijft leidend. Bij verschillen tussen deze vertaling en het originele Engelstalige rapport geldt uitsluitend de Engelse tekst.

SIVON is een aantal jaar geleden zelf een DPIA-onderzoek op HR2day gestart. Publicatie daarvan is destijds aangehouden in afwachting van de referentie-DPIA van SURF om dubbel werk en uitvoeringslast bij de leverancier te voorkomen. Hierdoor is er één actuele en gezaghebbende DPIA (in plaats van twee naast elkaar bestaande analyses). SIVON zal daarom geen vervolg geven aan het eerder gestarte DPIA-onderzoek en sluit voor de applicatie HR2day aan op de actuele uitkomsten van SURF. De DPIA ondersteunt de conclusie dat onderwijsinstellingen HR2day kunnen blijven gebruiken onder de voorwaarden dat de hoge risico's door HR2day worden gemitigeerd, de lokale DPIA door ieder individueel schoolbestuur wordt uitgevoerd en onderwijsinstellingen de voorgestelde maatregelen implementeren. Daarmee vormt deze vertaling een praktische ondersteuning bij het verantwoord gebruik van ict in het funderend onderwijs.

SIVON, 16 juni 2026

# Oplegger HR2day B.V. bij de referentie-DPIA HR2day – 10 april 2026

*Dit oplegvel vertegenwoordigt de visie van HR2day op de DPIA. Alle uitspraken, meningen of standpunten die in het oplegvel staan of die als onderdeel van de visie van HR2day zijn opgenomen, zijn uitsluitend toe te schrijven aan HR2day en weerspiegelen niet noodzakelijkerwijs de standpunten, bevindingen of conclusies van SURF.*

Datum: 10-04-2026

Van: HR2day B.V.

Aan: Onderwijsinstellingen (klanten HR2day), SURF

Betreft: Reactie op de referentie-DPIA HR2day (versie 1.0)

## Initiatief en waardering

HR2day heeft het initiatief genomen om SURF te benaderen voor het uitvoeren van deze referentie-DPIA. Het beschermen van de persoonsgegevens van onze klanten, waaronder veel onderwijsinstellingen, zien wij niet als een passieve verplichting, maar als een verantwoordelijkheid die wij proactief dragen. Dat wij als leverancier dit traject zelf hebben opgestart, onderstreept hoeveel belang we bij HR2day hechten aan transparantie en aan het continu verbeteren van onze dienstverlening op het gebied van privacy.

Wij waarderen de samenwerking met SURF en hebben gedurende het gehele traject actief meegewerkt met als doel maximale transparantie: we hebben documentatie gedeeld, vragen beantwoord, een testomgeving beschikbaar gesteld en technische medewerkers ingezet. Om SURF optimaal te ondersteunen bij deze DPIA, heeft HR2day externe expertise ingeschakeld, te weten adviesbureau Cuccibu. Wij hebben van SURF gedurende het traject op meerdere momenten positieve feedback gekregen over de medewerking aan deze DPIA.

De DPIA bevestigt dat HR2day een effectief instrument is voor personeels- en salarisadministratie en dat instellingen het systeem AVG-conform kunnen blijven gebruiken . HR2day committeert zich aan de uitvoering van de maatregelen die aan haar zijde zijn belegd.

## Kanttekeningen bij de risicobeoordeling

Bewijslast en feitelijke situatie. Verschillende risico's zijn gebaseerd op het uitgangspunt dat SURF bepaalde verwerkingen niet heeft kunnen uitsluiten, waarna deze als vaststaand risico zijn opgenomen. HR2day erkent dat op een aantal punten meer transparantie wenselijk is en neemt hiervoor concrete stappen. HR2day benadrukt dat er geen feitelijke aanwijzingen zijn dat HR2day of Salesforce persoonsgegevens verwerken buiten de contractueel vastgelegde afspraken in de verwerkersovereenkomsten. HR2day verwerkt applicatiedata uitsluitend als

verwerker namens de instellingen. Onze privacyverklaring — die in de DPIA wordt aangehaald — heeft enkel betrekking op onze eigen bedrijfsactiviteiten (zoals websitebezoek en marketing) en niet op de (persoons)gegevens in de HR2day-applicatie. Wij zullen onze privacyverklaring verduidelijken om elke onduidelijkheid weg te nemen.

Risico-inschalingen. Van de 18 geïdentificeerde risico's classificeert SURF er 17 als 'hoog'. Wij merken hierbij op dat een deel van deze risico's inherent is aan elk HRM-systeem of aan het gebruik van cloudplatformen in het algemeen, en dus niet specifiek is voor HR2day. Bovendien worden bestaande waarborgen — zoals onze ISAE 3402 Type II-certificering, de ISO 27001- en SOC 2-certificeringen van Salesforce, EU-regional hosting, encryptie in transit en at rest en het uitgebreide autorisatiemodel in de DPIA niet altijd volledig meegewogen. Wij adviseren instellingen om bij hun eigen risicobeoordeling ook dit uitgebreide stelsel van beveiligingsmaatregelen en de governance van het Visma Data Protection Programma, waar HR2day onderdeel van is, in ogenschouw te nemen.

Nuancering beoordeling cloudplatformen. De DPIA presenteert het gebruik van het Salesforce-platform overwegend als risicoverhogend, met name vanwege de omvang en de Amerikaanse oorsprong van Salesforce. HR2day merkt op dat de schaal van een wereldwijde marktleider juist ook aanzienlijke voordelen biedt die in de DPIA onderbelicht blijven: enterprise-grade beveiliging, continue investeringen in compliance-certificeringen (ISO 27001, SOC 2, C5 ISAE, BCR-P), een Data Privacy Framework-certificering. Bovendien biedt Salesforce data-hosting binnen de EU en een architectuur waarin klantdata en applicatielogica strikt gescheiden zijn. De bewuste keuze van HR2day voor Salesforce is mede ingegeven door deze hoogwaardige waarborgen, die naar onze mening essentieel zijn voor een evenwichtige risicobeoordeling.

Afstemming met Salesforce. HR2day is doorlopend in contact met Salesforce voor maximale transparantie over de aard van de zogenoemde 'Usage Data', inclusief de gehanteerde anonimiseringsmethoden en de reikwijdte van de Salesforce DPA. HR2day houdt de onderwijsinstellingen hierover graag op de hoogte en betrekt hen actief bij dit traject. Gezamenlijk stemmen we af welke aanvullende contractuele of technische maatregelen wenselijk zijn, waarna we de verwerkersovereenkomsten in nauwe afstemming met de onderwijsinstellingen zullen actualiseren.

### Concrete acties HR2day

Onafhankelijk van bovenstaande kanttekeningen heeft HR2day reeds de volgende stappen gezet of in gang gezet:

- Digital Trust & Compliance Manager: HR2day heeft een Digital Trust & Compliance Manager aangenomen die zich volledig richt op privacy, informatiebeveiliging en compliance. Deze aanstelling onderstreept dat HR2day de bescherming van (persoons)gegevens als structurele prioriteit beschouwt — niet als eenmalig project, maar als blijvend onderdeel van onze organisatie.

- Vervanging SignRequest: De transitie naar ValidSign (EU-gevestigd, onderdeel van Visma) was al vóór afronding van de DPIA in gang gezet.
- DPA Expo: HR2day heeft inmiddels een verwerkersovereenkomst met Expo afgesloten.
- Cookiestatement: Alle benodigde informatie over cookies is beschikbaar en wordt omgezet in een volledig cookiestatement voor de applicatie.
- Subverwerkerscommunicatie: HR2day richt een formeel proces in om wijzigingen in de subverwerkerlijst van Salesforce tijdig door te communiceren aan instellingen.
- Informatievelden bij open tekstvelden: HR2day heeft in haar ontwikkelcyclus opgenomen dat gebruikers van onderwijsinstellingen beter worden geïnformeerd over het beoogde gebruik van open tekstvelden, middels informatievelden en instructies. Dit is intern als actie opgenomen en reeds verwerkt in onze processen.
- User satisfaction: HR2day zal deze verwerking opnemen in de verwerkersovereenkomst en instellingen de mogelijkheid bieden om de functionaliteit uit te schakelen.
- Verwerkersovereenkomst: HR2day zal indien nodig de verwerkersovereenkomst conform het SURF-model aanpassen of middels een addendum de eventueel ontbrekende informatie opnemen. Dit doen wij graag gezamenlijk met de onderwijsinstellingen, daar zij als verwerkingsverantwoordelijke vaak initiatiefnemer zijn van de eerder gesloten verwerkersovereenkomst.

Wij zien deze DPIA als een waardevol instrument om de privacybescherming voor de medewerkers van de onderwijsinstellingen continu te versterken. Wij kijken dan ook uit naar de verdere samenwerking met SURF en de instellingen bij de implementatie van de maatregelen.

Namens HR2day B.V.

Marco Boerlage - Directeur

# Samenvatting

Dit rapport is een gegevensbeschermingseffectbeoordeling (hierna: DPIA) over 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 de beoordeling van gegevensbeschermingsrisico's binnen HR2day.

### Over de dienst

HR2day is een all-round HRM- en salarissysteem dat bestaat uit verschillende modules en de volledige medewerkerscyclus ondersteunt van onboarding tot offboarding en alles daartussenin. Het biedt standaardprocessen die kunnen worden aangepast voor gebruik door individuele instellingen en wordt gebruikt door zowel mbo-instellingen als hogescholen.

Als cloudgebaseerde SaaS-applicatie is HR2day gebouwd om native te draaien op het Salesforce-platform, waarbij gebruik wordt gemaakt van kerntechnologieën en -diensten van Salesforce voor een schaalbare HR-ervaring.

### Reikwijdte

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

- Personeels- en salarisadministratie
- Selfservice (ESS/MSS)
- Verlof
- Verzuim
- Declaraties
- Documentbeheer
- Rapportages
- Digitale handtekening
- HR-analytics
- Medewerkersfeedback
- "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 risico's die specifiek zijn voor individuele instellingen. In plaats daarvan wordt een meer algemene beoordeling gemaakt op basis van het beoogde gebruik van HR2day door instellingen. Instellingen die HR2day willen gebruiken, kunnen deze

DPIA als uitgangspunt gebruiken, maar moeten deze aanvullen, uitbreiden en/of aanpassen op basis van de specifieke context waarin zij HR2day willen inzetten.

### Methodologie

SURF heeft de volgende methoden gebruikt voor de beoordeling:

- Deskresearch 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 aangemaakt, inclusief gebruik van een gespecialiseerde monitoringtool (man-in-the-middle proxy).
- Inzageverzoeken (DSAR's), ingediend na het technisch onderzoek.
- Reviews door HR2day en SURF.

### Uitkomst: 16 hoge risico's en 2 nader te bepalen risico's

Deze DPIA heeft zestien hoge risico's voor betrokkenen geïdentificeerd en twee risico's waarvoor 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 de inrichting van HR2day. Twee risico's houden verband met het gebruik van de mobiele app. Deze twee risico's gelden voor elke app die gebruik maakt van een app store en pushmeldingen. Omdat SURF aanvullend onderzoek doet naar de impact van deze risico's, wordt het risiconiveau op een later moment bepaald.

Door de maatregelen te implementeren worden alle hoge risico's gemitigeerd en resteert slechts een laag restrisico. Hoewel het niet strikt noodzakelijk is om lage risico's te mitigeren, wordt dit wel aanbevolen.

Voor al deze risico's is een termijn opgenomen voor het implementeren van de maatregelen. Instellingen kunnen HR2day daarom blijven gebruiken. Als de hoge risico's zijn gemitigeerd, is voorafgaande raadpleging van de toezichthoudende autoriteit voor gegevensbescherming niet vereist. SURF zal in 2027 een actualisatie van deze DPIA publiceren met een conclusie over de implementatie van de resterende maatregelen.

Hieronder volgt een overzicht van alle geïdentificeerde risico's en voorgestelde maatregelen. De status van de maatregelen die HR2day moet nemen, is weergegeven in de rechterkolom[1].

| # | Risico | Maatregelen instelling | Maatregelen HR2day | Status HR2day-maatregel(en) |
|---|---|---|---|---|
| **Risico's gerelateerd aan het Salesforce-platform** | | | | |
| 16.1 | Verlies van controle en verlies van vertrouwelijkheid door ongeoorloofde toegang via doorgiften aan Salesforce | Neem alle rechtmatige doorgiften op in de verwerkersovereenkomst | Neem alle rechtmatige doorgiften op in de verwerkersovereenkomst | De deadline hiervoor is 31-12-2026. |
| 16.2 | Verlies van controle als gevolg van een gebrek aan transparantie over de verwerking van gebruiks-gegevens voor doeleinden Salesforce | Werk de verwerkersovereenkomst 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;<br>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 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 verwerkersovereenkomst.<br><br>Update verwerkersovereenkomst | De deadline hiervoor is 31-12-2026. |

[1] *Noot bij de Nederlandse vertaling:* om zo dicht mogelijk bij de teksten van SURF te blijven, is voor de vertaling van deze tabel gebruik gemaakt van de door SURF vertaalde samenvatting (“SURF 260512-Final-DPIA-HR2day-courtesy-translation”).

| # | Risico | Maatregelen instelling | Maatregelen HR2day | Status HR2day-maatregel(en) |
|---|---|---|---|---|
| | | | 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;<br>auditrecht voor instellingen met betrekking tot de verwerkersovereenkomst. | |
| 16.3 | Onvermogen om rechten van betrokkenen uit te oefenen op persoonsgegevens | | 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 over de verwerking van persoonsgegevens via cookies | | Volledige cookieverklaring verstrekken aan alle gebruikers die HR2day gebruiken. | HR2day zal de cookieverklaring uiterlijk op 1-8-2026 voltooien en de cookieverklaring opnemen in |

| # | Risico | Maatregelen instelling | Maatregelen HR2day | Status HR2day-maatregel(en) |
|---|---|---|---|---|
| | | | | 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 de maatregelen voor risico 16.2). |
| **Algemene risico's** | | | | |
| 16.6 | Verlies van controle door gebrek aan transparantie over de verwerking van persoonsgegevens voor doeleinden van HR2day | Werk de verwerkersovereenkomst 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; 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 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 verwerkersovereenkomst.<br><br>Update privacyverklaring HR2day. | De deadline hiervoor is 31-12-2026.<br><br>HR2day zal haar privacyverklaring uiterlijk 1-8-2026 bijwerken. |

| # | Risico | Maatregelen instelling | Maatregelen HR2day | Status HR2day-maatregel(en) |
|---|---|---|---|---|
| 16.7 | Verlies van controle over gebruikstevredenheidsdata | | HR2day neemt deze verwerking op in de verwerkersovereenkomst als verwerker en geeft instellingen zinvolle controle (door middel van transparantie) en keuzes bij deze verwerking. | HR2day zal dit uiterlijk op 31-12-2026 in de verwerkersovereenkomst opnemen en instellingen de mogelijkheid bieden deze functionaliteit uit te schakelen. |
| 16.8 | Verlies van controle en verlies van vertrouwelijkheid door ongeoorloofde toegang in derde landen | Stop met het gebruik van SignRequest. | Identificeer alle overdrachten, in ieder geval naar Expo en Google.<br><br>Neem rechtmatige doorgiften aan subverwerkers op in de verwerkersovereenkomst tussen HR2day en de instelling.<br><br>Informeer instellingen over de partijen waaraan persoonsgegevens worden doorgegeven en waarmee zij rechtstreeks overeenkomsten moeten sluiten.<br><br>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. | De deadline hiervoor is 31-12-2026.<br><br>De deadline hiervoor is 31-12-2026.<br><br>De deadline hiervoor is 31-12-2026.<br><br>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 |

| # | Risico | Maatregelen instelling | Maatregelen HR2day | Status HR2day-maatregel(en) |
|---|---|---|---|---|
| | | | | 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.<br><br>Neem Google en Apple op in de verwerkersovereenkomst tussen HR2day en de instellingen.<br><br>Sluit de benodigde overeenkomsten met Google en Apple. | De deadline hiervoor is 31-12-2026.<br><br>De deadline hiervoor is 31-12-2026.<br><br>De deadline hiervoor is 31-12-2026. HR2day streeft ernaar om uiterlijk op 1-8-2026 subverwerkersovereenkomsten te hebben gesloten met alle subverwerkers. |

| # | Risico | Maatregelen instelling | Maatregelen HR2day | Status HR2day-maatregel(en) |
|---|---|---|---|---|
| 16.10 | Verlies van vertrouwelijkheid door het ontbreken van 'leestoegangslogging' | Implementeer 'read access logging' op ten minste de categorieën gevoelige en bijzondere gegevens.<br><br>Implementeer logboekregistratie van leestoegang voor activiteiten die beheerders uitvoeren via de proxy-login.<br><br>Gebruikers onverwijld informeren dat er misbruik is gemaakt van hun identiteit. | 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. |
| 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.<br><br>Laat de keuzelijst voor verzuim en de vaste set velden beoordelen door de privacyafdeling[2], om er zeker van te zijn dat ze in overeenstemming zijn met de AVG-vereisten en de beschikbare richtlijnen. | | 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 voor deze maatregel is 31-12-2026. |

[2] Noot bij Nederlandse vertaling: de privacy officer, functionaris voor gegevensbescherming (FG), adviseur IBP of leden van het IBP-team

| # | Risico | Maatregelen instelling | Maatregelen HR2day | Status HR2day-maatregel(en) |
|---|---|---|---|---|
| | | 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 (verlies van controle door open tekstvelden) | 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 (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. | HR2day geeft aan dit in de ontwikkelingscyclus te hebben geïmplementeerd en veldvalidatie te tonen voor BSN-nummers en IBAN's. De |

| # | Risico | Maatregelen instelling | Maatregelen HR2day | Status HR2day-maatregel(en) |
|---|---|---|---|---|
| | | Zorg ervoor dat gebruikers van HR2day goed worden geïnstrueerd en getraind over welke soorten gegevens in open tekstvelden mogen worden verwerkt. | | deadline voor deze maatregel is 31-12-2026. |
| 16.13 | Gebrek aan juistheid door handmatige registratie van persoonsgegeve ns | Automatiseer de invoer waar mogelijk, bijvoorbeeld door HR2day te koppelen aan het wervingssysteem.<br><br>Zorg ervoor dat HR-medewerkers goed zijn geïnstrueerd en getraind in de procedures van de instellingen voor het zorgvuldig registreren van persoonsgegevens. | Zorg voor voldoende mogelijkheden voor veldvalidatie om onnauwkeurige gegevensverwerking te voorkomen. | HR2day geeft aan dit in de ontwikkelingscy clus te hebben geïmplementee rd en toont veldvalidatie voor bsn-nummers en IBAN's. De deadline voor deze maatregel is 31-12-2026. |
| 16.14 | Verlies van controle over bewaar-termijnen door gebrek aan automatisering en | Bepaal en beheer bewaartermijnen voor persoonsgegevens in HR2day.<br><br>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. | Geef instellingen informatie en instructies over de procedure voor het verwijderen van gegevens met behulp van signaallijsten.<br><br>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. | HR2day heeft contact met twee instellingen en werkt aan (i) het gewenste detailniveau van bewaartermijne n (generiek versus per gegevensgroep) en<br>(ii) de mate van uniformiteit tussen instellingen. De deadline voor |

| # | Risico | Maatregelen instelling | Maatregelen HR2day | Status HR2day-maatregel(en) |
|---|---|---|---|---|
| | | | | deze maatregelen is 31-12-2026. |
| 16.15 | Verlies van vertrouwelijk-heid door standaardins telling voor verticale overerving van rechten | Schakel de verticale overerving van rechten uit, tenzij het nodig is om deze instelling te gebruiken.<br><br>Beperk de toegang tot persoonsgegevens voor functies die deze gegevens niet nodig hebben om hun taken uit te voeren.<br><br>Wees transparant tegenover de betrokkenen over het gebruik van de instelling voor verticale overerving van rechten en over wie toegang heeft tot hun gegevens. | 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.<br><br>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 workflows uit te voeren terwijl de instelling is uitgeschakeld. | De deadline hiervoor is 31-12-2026. |
| 16.16 | Verlies van vertrouwelijk-heid 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 | 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 encryptiesleutels.<br><br>Samenwerken met instellingen bij het | Op 31-12-2026 zal HR2day aanvullende beveiligings-maatregelen voor instellingen beschikbaar stellen. De mogelijkheid voor instellingen om hun eigen encryptiesleute |

| # | Risico | Maatregelen instelling | Maatregelen HR2day | Status HR2day-maatregel(en) |
|---|---|---|---|---|
| | | beveiligingsmaatregelen die van kracht zijn. | beoordelen van het vereiste encryptiesniveau voor de persoonsgegevens in HR2day, met name voor de gevoelige en bijzondere categorieën persoonsgegevens.<br><br>Waar instellingen dit nodig achten, worden aanvullende beveiligingsmaatregelen geïmplementeerd, zoals encryptie op celneiveau en encryptiesleutels die door HR2day worden beheerd. | Is te beheren bestaat al. Daarnaast zal HR2day samen met instellingen een werkgroep opzetten om de gewenste opties te beoordelen. |
| **Risico's als gevolg van het aanbieden van een mobiele app via de app stores van Google en Apple** | | | | |
| 16.17 [3] | Verlies van controle over de verwerkte persoons-geg evens 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.<br><br>Voer evenredigheids- en subsidiariteits-beoordelingen uit met betrekking tot het aanbieden van de mobiele app via app-winkels en ‘side-loading’ en implementeer de resultaten. | Maak de app beschikbaar als sideload.<br><br>Maak toegang via de mobiele browser vanaf mobiele apparaten mogelijk. | HR2day zal contact opnemen met instellingen over hun wensen in dit verband. |
| 16.18 [3] | 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. |

[3] Noot bij de Nederlandse vertaling: aangezien SURF een aanvullend onderzoek uitvoert naar de impact van deze risico's, zal het risiconiveau op een later tijdstip worden bepaald.

| # | Risico | Maatregelen instelling | Maatregelen HR2day | Status HR2day-maatregel(en) |
|---|---|---|---|---|
| | | Voer evenredigheids- en subsidiariteits-beoordelingen uit met betrekking tot het verzenden van pushmeldingen via Google en Apple of Unified Push en implementeer de resultaten. | | |

# Inleiding

HR2day is een applicatie voor human resource management (HRM) en salarisadministratie, eigendom van het gelijknamige bedrijf. Het is een software-as-a-service (SaaS)-oplossing, ingezet op het Salesforce platform-as-a-service (PaaS). HR2day kan via een API verbinding maken met andere applicaties. In deze DPIA worden de verwerkingen van persoonsgegevens besproken die plaatsvinden bij het gebruik van HR2day.

### SURF

SURF[4] is de IT-coöperatie van onderwijs en onderzoek in Nederland. SURF is eigendom van haar leden, bestaande uit voornamelijk onderwijs- en onderzoeksinstellingen. Via SURF werken zij samen aan onder meer de inkoop van de best mogelijke digitale diensten en het ontwikkelen en delen van kennis met elkaar. Een onderdeel van de dienstverlening van SURF is het uitvoeren van DPIA's op IT-diensten die veel leden gebruiken.

### DPIA's

DPIA staat voor Data Protection Impact Assessment (gegevensbeschermingseffectbeoordeling) en deze moet worden uitgevoerd door verwerkingsverantwoordelijken wanneer zij persoonsgegevens verwerken op een wijze die "waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen", conform artikel 35 van de Algemene Verordening Gegevensbescherming (AVG). De beoordeling is bedoeld om onder meer licht te werpen op de specifieke verwerkingsactiviteiten, het inherente risico voor betrokkenen en de waarborgen die zijn toegepast om deze risico's te beperken. Het doel van een DPIA is te waarborgen dat eventuele risico's verbonden aan het betreffende proces in kaart zijn gebracht en beoordeeld, en dat adequate beveiligingsmaatregelen zijn getroffen om deze risico's te mitigeren.

Betrokkenen hebben een fundamenteel recht op bescherming van hun persoonsgegevens en andere fundamentele vrijheden die kunnen worden beïnvloed door de verwerking van persoonsgegevens, zoals de vrijheid van meningsuiting. Het recht op gegevensbescherming is daarmee breder dan het recht op privacy. Overweging 4 van de AVG luidt:

> *"Deze verordening eerbiedigt alle grondrechten en neemt de vrijheden en beginselen in acht die zijn erkend in het Handvest, zoals verankerd in de Verdragen, in het bijzonder de eerbiediging van het privéleven en het familie- en gezinsleven, de woning en de communicatie, de bescherming van persoonsgegevens, de vrijheid van gedachte, geweten en godsdienst, de vrijheid van meningsuiting en informatie, de vrijheid van ondernemerschap, het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, en de culturele, religieuze en taalkundige verscheidenheid."*

[4] Noot bij de Nederlandse vertaling: SIVON is de coöperatie van schoolbesturen in het funderend onderwijs en als sectororganisatie ondersteunt SIVON schoolbesturen bij het veilig en verantwoord inzetten van HR2day, onder andere door deze vertaling van de SURF-DPIA beschikbaar te stellen.

## Referentie-DPIA's versus individuele DPIA's

In AVG-termen is SURF niet de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens via het gebruik van HR2day. Elke individuele onderwijs- of onderzoeksinstelling die HR2day gebruikt, is de verwerkingsverantwoordelijke. Als IT-coöperatie van het Nederlandse onderwijs neemt SURF echter de verantwoordelijkheid op zich om de gegevensbeschermingsrisico's voor de eindgebruikers te beoordelen en te zorgen dat de gegevensverwerking voldoet aan de AVG. Daartoe voert SURF referentie-DPIA's uit om haar leden te helpen bij het selecteren van een privacyconforme implementatie en om waar nodig hun eigen DPIA's uit te voeren.

Alleen de organisaties zelf kunnen de specifieke gegevensbeschermingsrisico's beoordelen die verband houden met de technische privacyinstellingen, de aard en het volume van de verwerkte persoonsgegevens en de kwetsbaarheid van de betrokkenen. De Autoriteit Persoonsgegevens heeft deze aanpak onderschreven om de bescherming van persoonsgegevens in de onderwijssector te verbeteren.[1] Deze referentie-DPIA is bedoeld om onderwijs- en onderzoeksorganisaties te helpen bij de DPIA die zij moeten uitvoeren wanneer zij HR2day inzetten, maar kan de specifieke risicobeoordelingen die de organisaties zelf moeten maken niet vervangen.

Het uitvoeren van één referentie-DPIA voor een IT-dienst heeft voordelen voor de leden van SURF, maar ook voor de leveranciers van de door SURF beoordeelde producten. Voor de leden bespaart het de kosten van elk individueel het gehele DPIA-traject doorlopen. Zij kunnen ook hun gezamenlijke kennis over een product en ervaringen met een leverancier in de referentie-DPIA verwerken. Bovendien kan SURF effectiever onderhandelen over mitigerende maatregelen met de leveranciers, omdat het de gecombineerde onderhandelingskracht van de gehele sector als vertegenwoordiger heeft. Voor de leveranciers bespaart het eveneens tijd, inspanning en geld om niet elke instelling afzonderlijk bij DPIA's te hoeven begeleiden die naar verwachting grotendeels vergelijkbaar zullen zijn. Het is voor hen ook efficiënter om maatregelen te kunnen implementeren die alle leden tegelijk ten goede komen.

[1] Autoriteit Persoonsgegevens (alleen in het Nederlands), Sectorbeeld Onderwijs 2021-2023, 24 januari 2024, p. 5-6, URL: https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023.

## DPIA-criteria

De Autoriteit Persoonsgegevens (AP) heeft een lijst gepubliceerd van zeventien soorten verwerkingen waarvoor in Nederland altijd een DPIA verplicht is. Als een verwerking niet op deze lijst staat, moet een organisatie zelf beoordelen of de gegevensverwerking waarschijnlijk een hoog risico inhoudt. De Europese nationale toezichthoudende autoriteiten (hierna aangeduid als de gegevensbeschermingsautoriteiten of DPA's), verenigd in de European Data

Protection Board (EDPB), hebben ook een lijst met negen criteria gepubliceerd. Als vuistregel geldt dat een DPIA vereist is als een gegevensverwerking aan twee van deze criteria voldoet.

Van de EDPB-lijst zijn de criteria 4, 5 en 7 van toepassing, zoals dat waarschijnlijk geldt voor de meeste HR-systemen.

- Criterium 4 – Gevoelige gegevens of gegevens van zeer persoonlijke aard: Vanwege de aard van HR2day als HR-systeem bevat het bijzondere categorieën gegevens en gevoelige gegevens.
- Criterium 5 – Op grote schaal verwerkte gegevens: De persoonsgegevens in HR2day betreffen alle medewerkers en niet-bezoldigde personeelsleden van een instelling, en deze personen werken er mogelijk gedurende langere tijd, waardoor hun gegevens ook gedurende langere tijd worden verwerkt.
- Criterium 7 – Gegevens over kwetsbare betrokkenen: Er bestaat een machtsongelijkheid tussen werkgevers en werknemers.

### Reikwijdte

HR2day is ingedeeld in modules. Elke module bevat een bepaalde set functionaliteiten. In deze DPIA zijn de volgende modules onderzocht:

| Module | Functionaliteiten |
|---|---|
| Personeels- en salarisadministratie | Geautomatiseerde en nauwkeurige salarisadministratie en een volledig digitaal personeelsdossier en contractbeheer. |
| Selfservice (ESS/MSS) | ESS: Employee Interaction Centre, waar medewerkers hun eigen zaken kunnen beheren. MSS: Manager Interaction Centre, waar managers de zaken van hun teamleden kunnen beheren. |
| Verlof | Indienen van aanvragen voor en beheer van verlof in afstemming op het bedrijfsbeleid en cao's. |
| Verzuim | Beheer van verzuim wegens ziekte en andere redenen, alsmede ondersteuning voor communicatie met externe partijen zoals het UWV. |
| Declaraties | Indienen en beheren van declaraties. |
| Documentbeheer | Een digitaal dossier met alle documenten die betrekking hebben op medewerkers in de organisatie. |
| Rapportages | Genereren en exporteren van rapportages op basis van de gegevens in HR2day. |
| Digitale handtekening | Digitaal ondertekenen van (juridische) documenten. |
| HR-analytics | Biedt (real time) inzichten en analyses van HR-gegevens. |
| Medewerkersfeedback | Beheer en monitoring van de prestaties en ontwikkeling van medewerkers. |

| Module | Functionaliteiten |
|---|---|
| "Arbokoppeling" (API) | Maakt gegevensuitwisseling mogelijk tussen HR2day en systemen van arbodienstverleners. |

Het Salesforce-platform waarop HR2day is gebouwd, valt ook binnen de reikwijdte, aangezien het een integraal onderdeel is van de applicatie.

### Buiten reikwijdte

- De volgende modules zijn buiten de reikwijdte geplaatst vanwege het beperkte gebruik ervan door instellingen:
    - Opleidingsbeheer
    - 360 Graden feedback
    - Enquêtes
    - Portfolio
    - Formatie en budget
    - Sandbox
- Omdat de meeste mensen in de beroepsbevolking volwassenen zijn, gaat deze DPIA ervan uit dat de verwerking van persoonsgegevens van minderjarigen als gebruikers in HR2day een uitzondering is. Dit scenario valt buiten de reikwijdte van deze DPIA.

### Methodologie

Deze DPIA is tot stand gekomen via een combinatie van documentenonderzoek, technisch onderzoek en toelichtingen verstrekt door HR2day in reactie op vragen.

Het documentenonderzoek bestaat uit het opvragen en analyseren van overeenkomsten, beleidsdocumenten, procedures en informatiebeveiligingscertificeringen. HR2day kreeg ook de gelegenheid om op bevindingen te reageren, waarbij specifieke vervolgvragen werden gesteld. Dit onderdeel van het onderzoek richtte zich primair op de juridische afspraken die zijn gemaakt met betrekking tot de verwerking van gegevens in HR2day.

Het technisch onderzoek binnen de DPIA analyseert de technische aspecten van HR2day aan de hand van gebruiksscenario's.[2] Dit onderzoek sluit aan op de juridische bevindingen en onderzoekt hoe gegevens worden verzameld, verwerkt, opgeslagen, gedeeld en beveiligd. Technische analyse van gegevensstromen, opslagmethoden, logging, beveiligingsmaatregelen en privacyinstellingen wordt gebruikt om te beoordelen of de technische implementatie voldoet aan de AVG-vereisten:

- Intercepteren van netwerkverkeer tijdens het uitvoeren van testscenario's in de applicatie.
- Analyseren van technische documentatie.
- Analyseren van de gegevens die voortvloeien uit inzageverzoeken van betrokkenen.

De technische documentatie wordt eveneens bestudeerd en er zijn ook vragen gesteld aan HR2day in dit verband.

## Opzet

Deze DPIA is gebaseerd op het Nederlandse model-DPIA voor rijksdiensten.[3] Dit model is goed geschikt voor de activiteiten van onderwijs- en onderzoeksinstellingen, aangezien zij ook taken van algemeen belang uitvoeren. Omdat dit een referentie-DPIA is, zijn waar nodig wijzigingen aangebracht in de structuur van het oorspronkelijke model.

Het model bestaat uit vier delen.

- Deel A beschrijft de feiten van de gegevensverwerkingsactiviteiten;
- Deel B beoordeelt de rechtmatigheid van de in deel A beschreven feiten;
- Deel C behandelt de risico's voor de rechten en vrijheden van betrokkenen; en
- Deel D behandelt de maatregelen die zijn voorzien om deze risico's aan te pakken.

## Tijdlijn

Deze DPIA is gestart in januari 2025 en afgerond in mei 2026.

[2] Bijlage 1.1

[3] https://www.kcbr.nl/sites/default/files/2023-09/Model%20DPIA%20Rijksdienst%20v3.0.pdf, geraadpleegd op 6 mei 2025

# Deel A. Beschrijving van de verwerking

# 1 HR2day

HR2day is een all-round HRM-systeem dat een aantal processen ondersteunt met een vast datamodel. Dit betekent dat de structuur, velden en categorieën gegevens die klanten kunnen invoeren, volledig worden bepaald door HR2day. HR2day biedt standaardprocessen die kunnen worden aangepast voor gebruik door de individuele instelling.

Dit hoofdstuk dient als inleiding op het systeem. Het geeft een algemeen overzicht van de functionaliteiten, architectuur en componenten van het systeem, de van toepassing zijnde beveiligingscertificeringen en het bedrijf dat eigenaar is van het systeem.

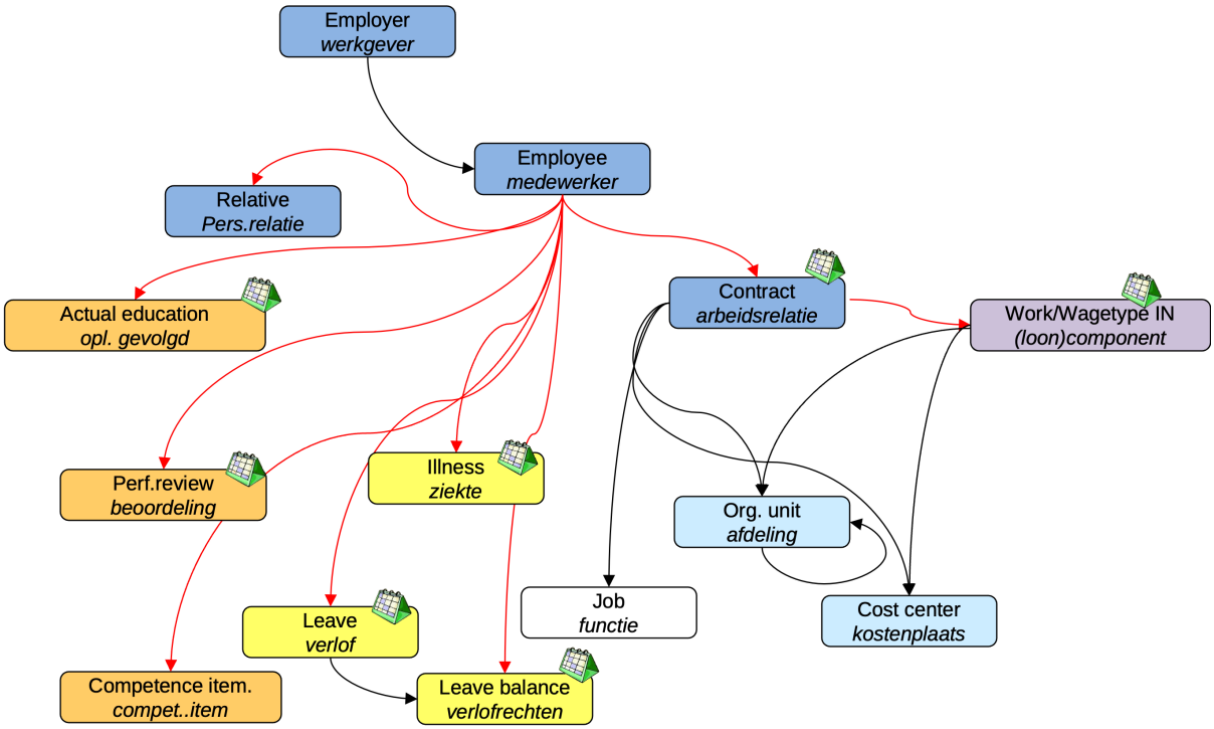
## 1.1 HR2day – HR en salaris in één applicatie

HR2day ondersteunt de volledige medewerkerscyclus van onboarding tot offboarding en alles daartussenin.

HR2day is gebouwd om flexibel en modulair te zijn; klanten kunnen het systeem (workflows) aanpassen aan hun behoeften en kiezen uit een breed scala aan modules om in hun behoeften te voorzien.

| Talent Management | Self Service | HR & Payroll | HR Analytics |
|---|---|---|---|
| Werving | Employee self service | Formatieplan en budgettering | Bedrijfsrapportage |
| Prestatiemanagement | Manager self service | Personeelsadministratie | Bedrijfsturing |
| Opleidingsbeheer | Workflows | Digitaal dossier | Business intelligence |
| Competentiemanagement | | Organisatiebeheer<br>Salarisverwerking | |
| Portfoliobeheer | | Verlof<br>Verzuim | |
| | | Declaraties | |

Tabel 1-1, HR2day-modules.[4]




Figuur 1-1, HR-data vs. payroll data from presentation HR2day.

HR2day is geconfigureerd op basis van cao-voorwaarden, waardoor clusters van arbeidsvoorwaarden kunnen worden aangemaakt om naleving van de betreffende cao te waarborgen. Het systeem koppelt ook medewerkergegevens aan hun arbeidsrelatie, waardoor deze relatie de fundamentele basis vormt voor het dossier van de medewerker binnen het systeem.

[4] Uit presentatie HR2day.

## 1.2 Salesforce-architectuur

HR2day is een cloudgebaseerde SaaS-applicatie, gebouwd om native te draaien op het Salesforce-platform, waarbij gebruik wordt gemaakt van kerntechnologieën en -diensten van Salesforce voor een schaalbare HR-ervaring. De diepe integratie met Salesforce is centraal voor het ontwerp. Vanwege het belang van het Salesforce-platform voor HR2day zal deze DPIA ook aandacht besteden aan de gegevensverwerking via Salesforce.

*"Native Force.com-applicaties zijn volledig gebouwd op het Force.com-platform. Deze native apps bevinden zich binnen de Salesforce-infrastructuur en worden gehost, beheerd en geleverd door salesforce.com."*[5]

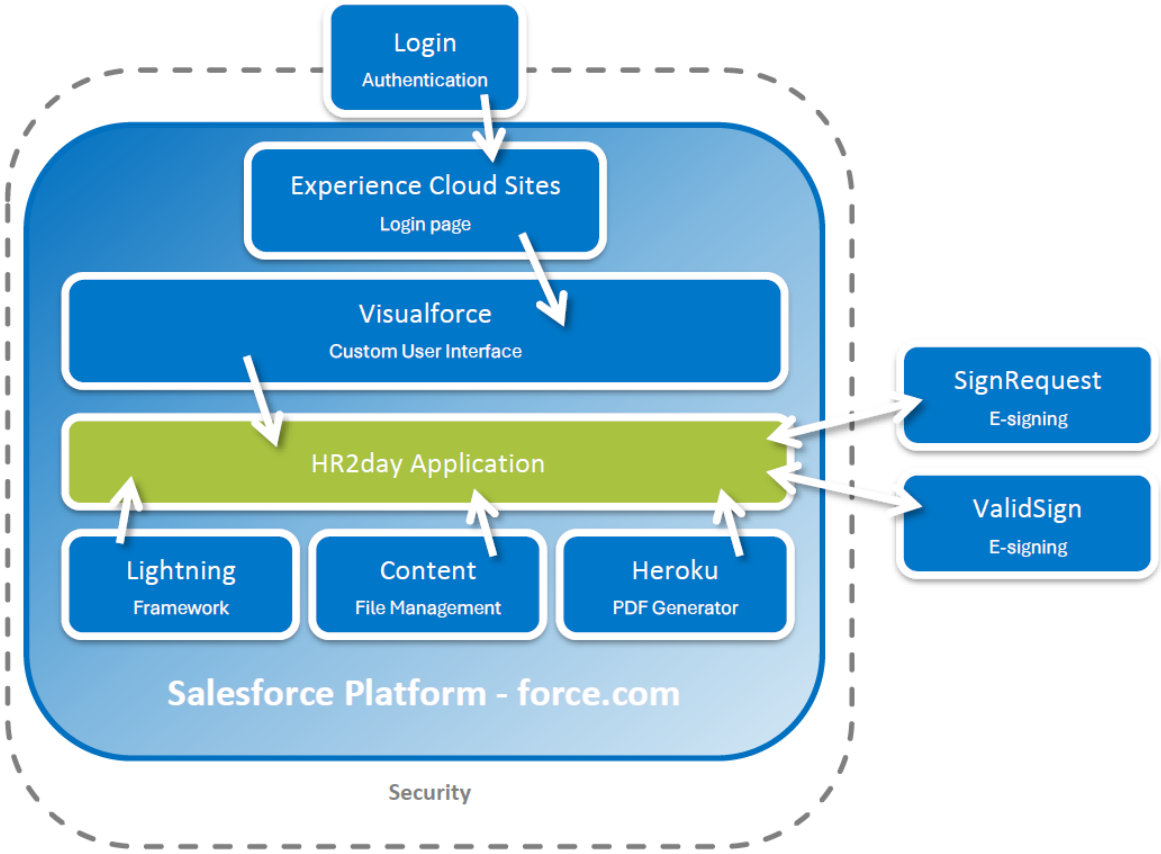
HR2day benadrukt dat het voor het Salesforce-platform heeft gekozen vanwege de beveiligingscertificeringen die Salesforce biedt. Zie voor meer informatie 1.3 Beveiliging.

[5] What is a Salesforce Native Application?, https://appexchange.salesforce.com/partners/servlet/servlet.FileDownload?file=00P3A00000RstvwUAB, geraadpleegd op 20 januari 2026.

### 1.2.1 Door HR2day gebruikte Salesforce-platformcomponenten

- Lightning biedt een consistente gebruikerservaring op desktop en mobiel, waarbij HR2day profiteert van de voortdurende ontwikkeling van deze dienst door Salesforce. Het is een op componenten gebaseerd framework voor app-ontwikkeling op het Salesforce-platform.
- Hyperforce is de volgende generatie infrastructuurfundament van Salesforce voor het inzetten van applicatiestacks op commerciële cloudproviders en stelt klanten in staat regio's te kiezen waar hun gegevens worden gehost.
- Login biedt authenticatie en gebruikersbeheer via de aanmeldings- en identiteitsservices van Salesforce. HR2day maakt gebruik van de beveiliging van Salesforce, inclusief single sign-on (SSO), meervoudige authenticatie (MFA) en gebruikersprovisioning.[6]
- Visualforce biedt een aangepaste gebruikersinterface. Dit maakt het mogelijk om op maat gemaakte workflows of formulieren te maken die verder gaan dan standaard Lightning-componenten.
- Content biedt bestandsbeheer voor het beheren van documenten, beleidsregels en personeelsdossiers. Dit omvat veilige, gecentraliseerde en beveiligde documentopslag met toegangscontroles.
- Experience Cloud Sites breidt het bereik uit naar externe gebruikers. In het geval van HR2day biedt het de aanmeldingspagina.
- Heroku voor het bouwen en uitvoeren van aangepaste applicaties (bijv. PDF-generator) of microservices die moeten communiceren met Salesforce-gegevens maar technologieën of frameworks vereisen die niet native door Salesforce worden ondersteund.

[6] Aanmaken, beheren, bijwerken en verwijderen van gebruikersaccounts en hun toegangsrechten.




Figuur 1-1 Schematic representation of architecture.

### 1.2.2 Beveiligingsraamwerk van Salesforce

HR2day maakt gebruik van de beveiligingsinfrastructuur van Salesforce, waaronder authenticatie, toegangscontroles en encryptie. Dit betekent dat de privacy en beveiliging van HR2day nauw verbonden zijn met de eigen compliancecertificeringen en -praktijken van Salesforce. Salesforce hanteert het Shared Responsibility Model, waarbij HR2day verantwoordelijk is voor het beveiligen van de HR2day-applicatie, die is gebouwd op het Salesforce-platform.[7]

[7] Security as a Shared Responsibility Between Provider and Customer, https://www.salesforce.com/blog/shared-responsibility-model/, geraadpleegd op 13 oktober 2025.

### 1.2.3 Complianceraamwerk van Salesforce

Salesforce biedt HR2day resources en documentatie die specifiek zijn bedoeld ter ondersteuning van DPIA's, zodat organisaties kunnen beoordelen hoe de technische en organisatorische maatregelen van Salesforce aansluiten bij de AVG en andere regelgeving op het gebied van gegevensbescherming.

HR2day kan gebruikmaken van de tools[8] van Salesforce voor inzageverzoeken van betrokkenen, gegevensexport en verwijdering.

[8] Salesforce help Data Protection and Privacy
https://help.salesforce.com/s/articleView?id=xcloud.data_protection_and_privacy.htm&type=5

## 1.3 Beveiliging

HR2day beschikt over een ISAE 3402 Type II-rapport met een carve-out voor de diensten van Salesforce. Salesforce heeft een ISO 27001-certificering en een SOC 2-rapport voor hun diensten op Hyperforce, waarop HR2day steunt en dat periodiek wordt gecontroleerd. Het op deze wijze regelen van beveiligingscertificeringen is een industriestandaard voor SaaS-aanbieders op platformdiensten.

## 1.4 HR2day+ App

HR2day gebruikt Salesforce als platform en publiceert haar mobiele applicatie genaamd HR2day+ respectievelijk op de Google Play Store en de Apple App Store. De app is een hybride app die een webview gebruikt om de HR2day-webapplicatie van het Salesforce-platform in een mobiele omgeving weer te geven. Dit betekent dat de app een native shell is die de door Salesforce gehoste webapplicatie laadt en weergeeft in een mobiele omgeving.

De mobiele applicatie maakt gebruik van dezelfde subverwerkers als zijn webgebaseerde tegenhanger en gebruikt één extra subverwerker voor het verzenden van notificaties (zie 4.4.3 Ontvangen van notificaties).

## 1.5 HR2day B.V.

HR2day B.V. is het bedrijf dat de applicatie HR2day exploiteert. Het bedrijf is voor 70% eigendom van Visma Nederland B.V., dat deel uitmaakt van de Europese Visma Group. De Visma Group is de moedermaatschappij van meer dan 200 dochterondernemingen zoals HR2day B.V. Het heeft een overkoepelende strategische rol en er zijn algemene kaders en richtlijnen opgesteld voor de dochterondernemingen. Het heeft een gelaagde hiërarchische organisatiestructuur waarin de dochterondernemingen operationele autonomie hebben, inclusief enige vrijheid op juridisch vlak.

Op het gebied van privacy is de autonomie echter beperkter en moeten dochterondernemingen voldoen aan de centrale richtlijnen en kaders die door de Visma Group zijn vastgesteld. Zo heeft de Visma Group een uitgebreid Data Protection Programme dat beleid, richtlijnen, risico- en volwassenheidsmonitoring, incidentafhandeling, bewustwording en verplichte privacytraining voor alle medewerkers omvat.[9]

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

[9] Data Protection Program, https://www.visma.com/trust-centre/privacy/data-protection-program, geraadpleegd op 13 oktober 2025.

# 2 Doeleinden

Dit hoofdstuk gaat over de doeleinden waarvoor HR2day persoonsgegevens van gebruikers verwerkt. Het opsommen van deze doeleinden geeft een algemeen beeld van waarvoor het product wordt gebruikt.

Een steekproef van verwerkersovereenkomsten van klanten van HR2day laat zien dat door klanten van HR2day vastgestelde doeleinden personeelsadministratie zijn, nader omschreven als "snelle en efficiënte toegang tot zowel individuele als collectieve personeelsinformatie [...] in het belang van een verantwoord personeelsbeleid voor zowel individuen als de organisatie als geheel" en het voldoen aan wettelijke vereisten.[10] Er is geen documentatie die expliciet aangeeft dat HR2day eigen doeleinden bepaalt voor de gegevensverwerking in HR2day als verwerker.

Naast deze in de verwerkersovereenkomsten gevonden doeleinden, zijn de onderstaande doeleinden gebaseerd op de contracten en aanbestedingsdocumentatie tussen HR2day en haar klanten, beschrijvingen van de verschillende HR2day-modules en het onderzoek naar de daadwerkelijke verwerkingsactiviteiten. Ze zijn onderverdeeld in doeleinden op basis van de functies zoals beschreven in het 'Hoger Onderwijs Referentie Architectuur'-model (HORA[5]) en overige doeleinden. De HORA is een bedrijfsfunctiemodel voor onderwijsinstellingen. Het beschrijft de functies van een organisatie, onafhankelijk van hoe deze functies zijn geïmplementeerd in een specifieke organisatie.[11] Omdat de HORA de essentiële functies van onderwijsorganisaties op een hoog niveau beschrijft, is het een goed model om de belangrijkste doeleinden voor gegevensverwerking in applicaties zoals HR2day van af te leiden. Het gebruik van de HORA als referentie zorgt er ook voor dat het voor instellingen gemakkelijk zal zijn om de juiste plek in hun organisatiestructuur te vinden voor de implementatie van eventuele maatregelen of wijzigingen uit deze DPIA. De andere categorie bestaat uit 'ondersteunende' doeleinden, die de hoofdprocessen ondersteunen.

[10] Verwerkersovereenkomst met [vertrouwelijk]; Verwerkersovereenkomst met [vertrouwelijk]; Verwerkersovereenkomst met [vertrouwelijk]. SURF-leden kunnen toegang vragen tot deze documenten.

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

## 2.1 HORA-doeleinden bepaald door de instellingen

De onderstaande doeleinden kunnen worden samengevat als personeels- en salarisadministratie.

### 2.1.1 Bedrijfsvoering – HRM

[5] Noot bij de Nederlandse vertaling: voor het funderend onderwijs kan gebruik worden gemaakt van de Funderend Onderwijs Referentie Architectuur (FORA): https://fora.wikixl.nl/index.php/FORA/id-40d06714-b4e1-41bb-84c5-befc54a1c734

HR2day is, zoals de naam al suggereert, een instrument ter ondersteuning van human resource- en salarisprocessen. De belangrijkste doeleinden van de verwerkingsactiviteiten in dit instrument zijn daarom gerelateerd aan HRM.

1. Formatieplan
Bepalen welke budgetten en functies beschikbaar zijn voor de afdelingen.

2. Medewerkerbeoordeling
Evalueren van medewerkersprestaties en nemen van beslissingen over beloning en promotie, alsmede ontslag en degradatie.

3. Medewerkeradministratie
Beheren van alle medewerkergegevens.

4. Salaris- en declaratieverwerking
Berekenen en uitbetalen van salarissen en declaraties van medewerkers.

5. Ziekte- en verlofadministratie
Registreren van ziekteverzuim en verlof van medewerkers.

### 2.1.2 Sturing – verantwoording

De informatie uit HR2day wordt ook gebruikt om inzicht te krijgen in het functioneren van de organisatie.

6. Interne rapportages Informatie over het functioneren van de organisatie beschikbaar stellen aan interne partijen.

## 2.2 Ondersteunende doeleinden bepaald door de instellingen

Instellingen gebruiken HR2day voor de doeleinden zoals beschreven in paragraaf 2.1. Om te waarborgen dat HR2day effectief, efficiënt en veilig functioneert, verwerkt HR2day persoonsgegevens voor de volgende doeleinden. Verwerkingsactiviteiten voor deze doeleinden zijn gebruikelijk voor IT-diensten, maar zijn niet gedefinieerd in enige documentatie van HR2day.

7. De dienst leveren en up-to-date houden
Uitvoeren van de handelingen die nodig zijn om te waarborgen dat de dienst continu en zoals bedoeld functioneert, zoals opslag, hosting, het verhelpen van bugs, etc.

8. De dienst beveiligen
Waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens in de dienst en de weerbaarheid van de dienst, onder andere door het faciliteren van identificatie en authenticatie en het maken van back-ups.

9. De dienst personaliseren
Ondersteunen van individuele gebruikersvoorkeuren en efficiënte informatievoorzienig.

10. Klantenondersteuning bieden
Bieden van methoden waarmee klanten en gebruikers ondersteuning kunnen vragen en ontvangen bij problemen.

11. De dienst verbeteren
Wijzigingen aanbrengen in de dienst in overeenstemming met de wensen van klanten.

## 2.3 Doeleinden bepaald door HR2day

HR2day heeft haar privacyverklaring met SURF gedeeld voor deze DPIA. Daarin staat niet expliciet vermeld of deze verklaring van toepassing is op persoonsgegevens die via de HR2day-applicatie worden verzameld of niet, maar wel dat HR2day gegevens kan verzamelen van betrokkenen die werken voor klanten van HR2day. Deze groep omvat gebruikers van de applicatie. HR2day heeft aangegeven dat deze verklaring niet van toepassing is op de HR2day-applicatie, met uitzondering van de verwijzing naar het aanmaken van accounts.[12]

In hun privacyverklaring bepaalt HR2day een aantal doeleinden waarvoor zij persoonsgegevens verwerken:

Aankoop en levering

- Faciliteren van klantorders, overeenkomsten, betalingen
- Rechtstreeks aanbieden van diensten aan u, zoals e-learning, webinars en rapporten enz.
- Op verzoek aan Klanten verstrekken van offertes voor producten en diensten
- Aanmaken en faciliteren van accounts voor gebruikers van onze diensten

Ondersteuning en verbetering

- Verbeteren en (verder) ontwikkelen van de kwaliteit, functionaliteit en gebruikerservaring van onze producten, diensten en de site van HR2day
- Aanbieden van klantondersteuning voor onze producten en diensten
- Exploiteren van gebruikerscommunities voor opleidingsdoeleinden en het mogelijk maken van interactie tussen gebruikers en HR2day

Beveiliging

- Opsporen, verhelpen en voorkomen van bedreigingen voor en misbruik van de beveiliging, uitvoeren van onderhoud en verwijderen van bugs

Marketing

- Beheren van marketingvoorkeuren en sturen van marketingcontent
- Aanmaken van belangstellingsprofielen voor het promoten van relevant producten en diensten (profilering)

Recruitment

- Het beheer van recruitment processen en het verwerken van sollicitaties
- Ingediende documenten evalueren, sollicitatiegesprekken voeren en referenties opvragen"[13]

[12] Opmerking op hoofdstuk 2.3 uit review, 21 november 2025.

[13] HR2day Privacy Statement, met SURF gedeeld op 20 maart 2025.

# 3 Persoonsgegevens

Conform artikel 4(1)(a) van de AVG:

> *"'persoonsgegevens': alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon."*

## 3.1 Categorieën betrokkenen

Als HR-systeem verwerkt HR2day de volgende categorieën betrokkenen:

- Medewerkers[14]
- Niet-bezoldigde personeelsleden
- Voormalige medewerkers en niet-bezoldigde personeelsleden
- Beheerders
- Docenten
- Partners / kinderen van (ex-)medewerkers

Omdat de meeste mensen in de beroepsbevolking volwassenen zijn, gaat deze DPIA ervan uit dat de verwerking van persoonsgegevens van minderjarigen als gebruikers in HR2day een uitzondering is. Dit scenario valt buiten de reikwijdte van deze DPIA. Een andere manier waarop gegevens van minderjarigen kunnen worden verwerkt, is wanneer de namen van kinderen van medewerkers worden geregistreerd.

[14] Voor de beknoptheid omvat de term "medewerkers" in de lopende tekst ook niet-bezoldigde personeelsleden en voormalige medewerkers en niet-bezoldigde personeelsleden. Als label verwijst "medewerkers" alleen naar werknemers die bij een werkgever in dienst zijn.

## 3.2 Verwerkte persoonsgegevens

### 3.2.1 Inzageverzoek betrokkenen

Als onderdeel van het technisch onderzoek zijn inzageverzoeken (Data Subject Access Requests, DSAR's) ingediend bij de leverancier. Deze verzoeken hadden betrekking op drie betrokkenen – twee medewerkers en één HR-manager – van wie de profielen zijn gebruikt om verschillende scenario's binnen het systeem uit te voeren.

#### 3.2.1.1 Door de leverancier verstrekte gegevens

De leverancier heeft de volgende gegevens verstrekt in reactie op de DSAR's:

- Overzicht van arbeidsrelaties
- Registratie van wijzigingen in arbeidsrelaties

- Log van aanmeldingsactiviteiten
- Persoonlijke gegevens van de medewerker
- Wijzigingslogs van persoonlijke medewerkergegevens
- Opleidingsgegevens
- Salarisspecificaties
- Salariscomponenten
- Rechtsgrondslag voor elke gegevenscategorie
- Lijst van derde partijen met wie gegevens worden gedeeld
- Bewaartermijnen per categorie persoonsgegevens
- Instructies voor betrokkenen over hoe zij toegang kunnen krijgen tot hun eigen informatie en deze kunnen bijwerken (inclusief toelichting dat bepaalde gegevens niet kunnen worden gewijzigd vanwege wettelijke verplichtingen)

#### 3.2.1.2 Belangrijkste bevindingen uit de DSAR-gegevensanalyse

Na analyse van de verstrekte gegevens zijn de volgende observaties gedaan:

- Gegevens ingediend/verwerkt door SignRequest (zie 4.3.6.1) ontbreken.
- Beveiligingsgerelateerde loggegevens ontbreken.
- Loggegevens bedoeld voor productontwikkeling ontbreken.
- De categorieën persoonsgegevens komen niet overeen met die in de steekproef van verwerkersovereenkomsten.[15]

[15] SURF heeft zijn technische tests in een eigen omgeving uitgevoerd, zodat de VWO's van de instellingen niet van toepassing zijn op deze tests. HR2day heeft echter zijn standaard DSAR-respons gebruikt met zijn standaard gegevenscategorieën, die de instellingen ook zouden ontvangen als ze een DSAR zouden doorsturen.

### 3.2.2 Categorieën persoonsgegevens

Voor deze DPIA zijn de persoonsgegevens in HR2day ingedeeld in categorieën. Elke categorie bevat persoonsgegevens die een vergelijkbare aard hebben. Zie Bijlage 2 voor een beschrijving van de categorieën. Sommige persoonsgegevens kunnen in meerdere categorieën vallen. In dat geval worden ze gecategoriseerd in de categorie met de hoogste gevoeligheid.

In de onderstaande tabellen zijn sommige gegevensitems van een vergelijkbaar type samengebracht in subgroepen voor beknoptheid. Zo bevat de subgroep 'Naam' de naam waarmee iemand aangesproken wordt, voornaam, achternaam, initialen, roepnaam en voorvoegsels. Evenzo bevat de categorie 'Salarisgegevens' verschillende soorten gegevens met verschillende gevoeligheidsniveaus. Voor het volledige overzicht van persoonsgegevensitems kan contact worden opgenomen met SURF Vendor Compliance.

Paragrafen 3.2.3 en 3.2.4 bevatten toelichtingen op de categorisering van bijzondere categorieën persoonsgegevens en gevoelige persoonsgegevens.

De onderstaande tabellen bevatten alle gegevensvelden die HR2day aanbiedt. Instellingen kunnen bepalen welke velden zichtbaar zijn voor gebruikers in de modules voor personeels- en salarisadministratie en verzuim.

| Direct identificeerbare persoonsgegevens | | | |
|---|---|---|---|
| **Persoonsgegevens** | **Betrokkene(n)** | **Gevoeligheid** | **Bron** |
| Naam | Medewerkers, Docenten, Partner / kind van (ex-)medewerker, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |
| Geboortedatum | Medewerkers, Docenten, Partner / kind van (ex-)medewerker, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |
| Geboorteplaats | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Bijzonder (in combinatie met nationaliteit) | Betrokkene of andere gebruikers van het systeem |
| ID-gegevens | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Bankgegevens | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Gebruiker | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Handtekening | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| ID-nummer | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Medewerkernummer | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| IBAN | Medewerkers, Ex-medewerkers, Docenten | Normaal | Betrokkene of andere gebruikers van het systeem |
| Foto | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |

| | | | |
|---|---|---|---|
| Nationaal identificatienummer | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Gevoelig | Betrokkene of andere gebruikers van het systeem |

| **Contactgegevens** | | | |
|---|---|---|---|
| **Persoonsgegevens** | **Betrokkene(n)** | **Gevoeligheid** | **Bron** |
| Adres | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| E-mailadres | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Telefoonnummer | Medewerkers, Docenten, Partner / kind van (ex-)medewerker, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Postcode | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |

| **Demografische gegevens** | | | |
|---|---|---|---|
| **Persoonsgegevens** | **Betrokkene(n)** | **Gevoeligheid** | **Bron** |
| Titel | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Geslacht | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Leeftijd | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| AOW-datum | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Nationaliteit | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Bijzonder (in combinatie met land/geboorteplaats) | Betrokkene of andere gebruikers van het systeem |

| | | | |
|---|---|---|---|
| Geboorteland | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Bijzonder (in combinatie met nationaliteit) | Betrokkene of andere gebruikers van het systeem |
| Burgerlijke staat | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Opleiding | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Arbeidsverleden | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Relatietype | Medewerkers, Docenten, Partner / kind van (ex-)medewerker, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |

| **Organisatorische gegevens** | | | |
|---|---|---|---|
| **Persoonsgegevens** | **Betrokkene(n)** | **Gevoeligheid** | **Bron** |
| Contractuele gegevens | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Afdeling | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Werklocatie | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Functie | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Deeltijdfactor | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Nevenwerkzaamheden | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal, mogelijk gevoelig of bijzonder | Betrokkene of andere gebruikers van het systeem |

| | | | |
|---|---|---|---|
| Eigenaar account | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Beoordelingen | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal, mogelijk gevoelig of bijzonder | Betrokkene of andere gebruikers van het systeem |
| Afspraken opleiding | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Competenties | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Verzuimgegevens | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Verlofgegevens | Medewerkers, Docenten, Niet-bezoldigde personeelsleden | Normaal | Betrokkene of andere gebruikers van het systeem |
| Betalingen | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |
| Contractuele gegevens | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |
| Documenten | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |
| Notities | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal, mogelijk gevoelig of bijzonder | Betrokkene of andere gebruikers van het systeem |
| Arbeidsrelatie | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |
| Activiteiten | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |

| | | | |
|---|---|---|---|
| Evenementen | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |
| Gespreksverslagen | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal, mogelijk gevoelig of bijzonder | Betrokkene of andere gebruikers van het systeem |
| E-mails | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |
| Salarisgegevens | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |
| Verzekeringsgegevens | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |
| Loonbeslag | Medewerkers, Docenten, Niet-bezoldigde personeelsleden, Ex-medewerkers | Normaal | Betrokkene of andere gebruikers van het systeem |

| **Gezondheidsgegevens** | | | |
|---|---|---|---|
| **Persoonsgegevens** | **Betrokkene(n)** | **Gevoeligheid** | **Bron** |
| Verzuimgegevens | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Bijzonder | Betrokkene of andere gebruikers van het systeem |
| Belastinggegevens | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Bijzonder | Betrokkene of andere gebruikers van het systeem |
| Salarisgegevens | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Bijzonder | Betrokkene of andere gebruikers van het systeem |
| Pensioengegevens | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Bijzonder | Betrokkene of andere gebruikers van het systeem |
| Uitkeringen | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Bijzonder | Betrokkene of andere gebruikers van het systeem |

| | | | |
|---|---|---|---|
| Arbeidsrelatie | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Bijzonder | Betrokkene of andere gebruikers van het systeem |

| **Financiële gegevens** | | | |
|---|---|---|---|
| **Persoonsgegevens** | **Betrokkene(n)** | **Gevoeligheid** | **Bron** |
| Salarisgegevens | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Gevoelig | Betrokkene of andere gebruikers van het systeem |
| Declaraties | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Gevoelig | Betrokkene of andere gebruikers van het systeem |
| Documenten | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Gevoelig | Betrokkene of andere gebruikers van het systeem |
| Contractuele gegevens | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Gevoelig | Betrokkene of andere gebruikers van het systeem |
| Reisgegevens | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Gevoelig | Betrokkene of andere gebruikers van het systeem |
| Loonbeslag | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Gevoelig | Betrokkene of andere gebruikers van het systeem |
| Arbeidsrelatie | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Gevoelig | Betrokkene of andere gebruikers van het systeem |
| Uitkeringen | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Gevoelig | Betrokkene of andere gebruikers van het systeem |
| Pensioengegevens | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Gevoelig | Betrokkene of andere gebruikers van het systeem |
| Lijfrente | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Gevoelig | Betrokkene of andere gebruikers van het systeem |

| **Vakbondsgegevens** |
|---|

| Persoonsgegevens | Betrokkene(n) | Gevoeligheid | Bron |
|---|---|---|---|
| Salarisgegevens (verrekening vakbondsbijdragen) | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Bijzonder | Betrokkene of andere gebruikers van het systeem |

| **Politieke gegevens** | | | |
|---|---|---|---|
| **Persoonsgegevens** | **Betrokkene(n)** | **Gevoeligheid** | **Bron** |
| Salarisgegevens (politiek verlof) | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden | Bijzonder | Betrokkene of andere gebruikers van het systeem |

**Technische/diagnostische/loggegevens**

Omdat dit een referentie-DPIA is die zich primair richt op risico's die inherent zijn aan het gebruik van de dienst die de leverancier aanbiedt, zijn de technische/diagnostische/loggegevens die leveranciers gewoonlijk verzamelen van bijzonder belang. De verwerking van deze gegevens kan op de achtergrond plaatsvinden zonder dat gebruikers en beheerders dit kunnen weten, wat een gebrek aan transparantie kan veroorzaken. De onderstaande tabel toont de technische/diagnostische gegevens die het onderzoek voor deze DPIA heeft aangetoond. Omdat de respons op de DSAR's echter onvolledige informatie bevatte, is de volledigheid van deze dataset niet geverifieerd.

| Persoonsgegevens | Betrokkene(n) | Gevoeligheid | Bron |
|---|---|---|---|
| Logging[16] | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden, Beheerders | Normaal | Systeem |
| Via cookies verzamelde gegevens[17] | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden, Beheerders | Normaal | Betrokkene, systeem |
| Apparaatgegevens | Medewerkers, Ex-medewerkers, Docenten, Niet-bezoldigde personeelsleden, Beheerders | Normaal | Systeem |

[16] Zie bijlage 1.5 voor de volledige lijst van gelogde gegevens.

[17] Zie bijlage 1.4 voor de volledige lijst van cookies.

### 3.2.3 Bijzondere categorieën persoonsgegevens

Artikel 9 van de AVG verbiedt de verwerking van bijzondere categorieën persoonsgegevens, die bestaan uit persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakvereniging blijken, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, of gegevens met betrekking

tot iemands seksueel gedrag of seksuele gerichtheid. Deze typen persoonsgegevens mogen alleen worden verwerkt als een van de uitzonderingen van artikel 9 lid 2 van toepassing is.

De meeste bijzondere categorieën persoonsgegevens in HR2day zijn gezondheidsgegevens. Instellingen kunnen in HR2day registreren wanneer medewerkers afwezig zijn, bijvoorbeeld wegens ziekte of zwangerschap, en de gegevens over de ziekte classificeren. Zij kunnen hun eigen categorieën hiervoor bepalen. HR2day biedt geen velden om de oorzaak van de ziekte te registreren.[18]

De ziekte van medewerkers beïnvloedt ook hun ziekengeld en daarmee hun salaris. Verder bevat HR2day gegevens over gebruikers die in aanmerking komen voor bepaalde uitkeringen, belastingvoordelen of arbeidsvoorzieningen wegens ziekte of arbeidsongeschiktheid. Bepaalde typen belastinggegevens, salarisgegevens, pensioengegevens en gegevens over de arbeidsrelatie kwalificeren daarmee als gezondheidsgegevens.

HR2day kan ook politieke gegevens en vakbondsgegevens bevatten. Werkgevers kunnen politiek verlof verlenen en vakbondsbijdragen voor medewerkers verrekenen, wat gevolgen heeft voor hun salaris.

Verder tonen nationaliteit in combinatie met geboorteplaats, geboorteland en foto de raciale of etnische afkomst van een betrokkene en vormen daarmee een bijzondere categorie persoonsgegevens.[19]

Ten slotte kunnen beoordelingen, notities, gespreksverslagen en nevenwerkzaamheden bijzondere categorieën persoonsgegevens bevatten, afhankelijk van wat door de instelling is geregistreerd. Zo kunnen deze velden notities bevatten over de activiteiten van medewerkers voor een politieke partij, notities over hoe de gezondheid van iemand zijn prestaties beïnvloedt, notities over de behoeften van iemand om zijn geloof op het werk te belijden, of notities over medewerkers die zich op het werk gediscrimineerd voelen vanwege hun seksuele gerichtheid. Vanwege de aard van deze velden is er een reële mogelijkheid dat dergelijke typen gegevens worden verwerkt.

[18] Zie Beleidsregels verwerking persoonsgegevens gezondheid zieke werknemers (https://wetten.overheid.nl/BWBR0037896/2016-04-29, geraadpleegd op 23 januari 2026) voor informatie over welke gegevens werkgevers mogen registreren over zieke medewerkers.

[19] Autoriteit Persoonsgegevens, Personeelsdossier, https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/personeelsgegevens/personeelsdossier, geraadpleegd op 16 oktober 2025.

### 3.2.4 Gevoelige persoonsgegevens

Sommige persoonsgegevens zijn niet bijzonder in de zin van artikel 9, maar kunnen gevoelig zijn vanwege hun relatief grote impact op iemands privacy.[20] Alle persoonsgegevens die informatie over iemands financiële situatie onthullen, kwalificeren als gevoelig.

Er is veel financiële data in HR2day, voornamelijk over het salaris van medewerkers. HR2day kan ook worden gebruikt om te registreren hoe de arbeidsrelatie tussen medewerkers en hun werkgevers gevolgen heeft voor hun salaris, hoe het pensioen van medewerkers wordt

beïnvloed door bepaalde omstandigheden, of er loonbeslag is gelegd op iemands salaris en of iemand uitkeringen ontvangt.

Beoordelingen, notities, gespreksverslagen en nevenwerkzaamheden kunnen vanwege de aard van deze velden ook gevoelige gegevens bevatten. Ze kunnen informatie bevatten die medewerkers delen met hun managers, maar die zij niet comfortabel zouden vinden om te delen met andere mensen. Voorbeelden zijn informatie over hun thuissituatie, de gezondheid van familieleden en financiële problemen.

Ten slotte kunnen gebruikers documenten zonder beperking uploaden en vanwege de aard van HR2day als HRM-systeem is er een mogelijkheid dat documenten gevoelige gegevens bevatten. Een voorbeeld zijn declaraties, die informatie bevatten over de financiële situatie van medewerkers.

[20] Autoriteit Persoonsgegevens, Wat zijn persoonsgegevens?, https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacy-en-persoonsgegevens/wat-zijn-persoonsgegevens#gevoelige-persoonsgegevens, geraadpleegd op 13 oktober 2025.

### 3.2.5 Nationaal identificatienummer

Werkgevers kunnen nationale identificatienummers in HR2day registreren. Zij zijn verplicht deze voor belastingdoeleinden te registreren en mogen deze alleen verwerken in overeenstemming met de Wet op de loonbelasting 1964.[21]

[21] BSN op het werk, https://www.autoriteitpersoonsgegevens.nl/en/themes/identification/citizen-service-number-bsn/bsn-at-work, geraadpleegd op 13 oktober 2025.

## 3.3 Bronnen van persoonsgegevens

Conform artikel 13 en 14 van de AVG moeten betrokkenen worden geïnformeerd over de verwerking van hun persoonsgegevens, ongeacht of deze rechtstreeks bij hen zijn verzameld. De persoonsgegevens in HR2day kunnen uit verschillende bronnen afkomstig zijn. Het is mogelijk om HR2day te koppelen aan een wervingssysteem, zodat (een deel van) de gegevens automatisch vanuit dat systeem kan worden geïmporteerd. Gebruikers kunnen ook handmatig persoonsgegevens invoeren over (nieuwe) medewerkers, hetzij over zichzelf, hetzij over andere medewerkers. De persoonsgegevens in HR2day worden derhalve geïmporteerd vanuit een wervingssysteem, rechtstreeks verzameld van de gebruikers, ingevoerd door andere gebruikers van het systeem, of gegenereerd op basis van gegevens die al aanwezig zijn in het systeem of het gedrag van gebruikers.

# 4 Verwerkingsactiviteiten

Dit hoofdstuk beschrijft de verwerkingsactiviteiten die kunnen plaatsvinden in HR2day. Conform artikel 4 lid 2 AVG wordt verwerking als volgt gedefinieerd:

> *"'verwerking': een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens."*

De verwerkingsactiviteiten zoals beschreven in de verwerkersovereenkomsten zijn "de verwerking van persoonsgegevens in het kader van salaris- en personeelsadministratie". De onderstaande beschrijvingen gaan nader in op de daadwerkelijke verwerkingsactiviteiten zoals gevonden in het onderzoek voor deze DPIA.

De bouwstenen van HR2day zijn processen. In HR2day nemen deze processen de vorm aan van workflows. Ze worden gedefinieerd door de typen activiteiten en acties die instellingen op gegevens kunnen uitvoeren, zoals indienen en goedkeuren/afwijzen. Dit deel van de verwerkingsactiviteit kan worden omschreven als het 'hoe'. Binnen het datamodel van HR2day zijn instellingen vrij om te bepalen welke typen gegevens ze in deze processen willen gebruiken. Dit deel van de verwerkingsactiviteit kan worden omschreven als het 'wat'. De verwerkingsactiviteiten voor verschillende instellingen kunnen er dus anders uitzien op basis van hoe zij de processen die HR2day aanbiedt hebben geïmplementeerd, hoewel sommige processen minder flexibel zijn dan andere. Dit hoofdstuk beschrijft het 'hoe', dus de verschillende processen die HR2day aanbiedt. Het beschrijft ook de persoonsgegevens die worden verwerkt in sommige processen in de standaardconfiguratie (het 'wat'). Het is echter belangrijk om in gedachten te houden dat de persoonsgegevens, zoals beschreven in hoofdstuk 3, die instellingen verwerken via de processen van HR2day kunnen afwijken van de standaardconfiguratie.

Dit hoofdstuk gebruikt labels om de relaties weer te geven tussen de processen en de andere componenten van deze DPIA, zoals de typen persoonsgegevens en de doeleinden.

## 4.1 Verzamelen

### 4.1.1 Onboarding

| | |
|---|---|
| **Doeleinden** | Authenticatie \| Medewerkeradministratie \| Salaris- en declaratieverwerking |
| **Gegevens** | Direct identificeerbaar \| Financieel \| Organisatorisch \| Etc. |
| **Gevoeligheid** | Normaal \| Gevoelig |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden |

Onboarding, of het aanmaken van nieuwe medewerkers in HR2day, kan plaatsvinden via een workflow (zie paragraaf 4.3.2), maar het is ook mogelijk dit 'handmatig' te doen. Deze workflow is opgenomen in de standaardinrichting van HR2day. Om een nieuwe medewerker in HR2day aan te maken, maakt een manager eerst een nieuwe "arbeidsrelatie" aan om alle persoonsgegevens over de nieuwe medewerker, zijn/haar rol in de organisatie en zijn/haar arbeidsvoorwaarden in te vullen. Alle gegevens over de nieuwe medewerker onder de "arbeidsrelatie" worden vervolgens automatisch gekopieerd naar het dossier onder "HR gegevens". De informatie over de "arbeidsrelatie" maakt ook deel uit van de "HR gegevens".

Daarna wordt een gebruikersaccount aangemaakt zodat de medewerker HR2day kan gebruiken en er wordt een profiel aan de gebruiker toegewezen. Dit verloopt halfautomatisch. Alle gegevens worden standaard overgenomen uit de medewerkergegevens, waarna de beheerder het juiste profiel moet selecteren. De rechten die een gebruiker in HR2day krijgt, zijn gebaseerd op het profiel. (Zie hoofdstuk 4.3.9 Beheer van rollen en profielen voor meer informatie over de rechtenstructuur.) Het is ook mogelijk om aanvullende rollen aan medewerkers toe te wijzen, die bepalen welke andere medewerkers voor de gebruiker zichtbaar zijn. Zo kunnen managers van een afdeling alle medewerkergegevens inzien van de medewerkers in die afdeling.

## 4.2 Opslaan van gegevens

| | |
|---|---|
| **Doeleinden** | Authenticatie \| Medewerkeradministratie \| Salaris- en declaratieverwerking |
| **Gegevens** | Direct identificeerbaar \| Financieel \| Organisatorisch \| Etc.[22] |
| **Gevoeligheid** | Normaal \| Gevoelig |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden |

Vrijwel alle gegevens in HR2day worden opgeslagen in datacenters in Frankrijk en Duitsland. Zie hoofdstuk 9 voor meer informatie hierover.

Gegevens die worden verwerkt door subverwerker SignRequest worden verwerkt in de VS.

[22] In plaats van alle categorieën op te sommen, wordt "Etc." gebruikt om aan te geven dat alle typen gegevens betrokken zijn.

## 4.3 Gebruik

### 4.3.1 Aanmelden/afmelden

| | |
|---|---|
| **Doeleinden** | De dienst beveiligen |
| **Gegevens** | Direct identificeerbaar \| Organisatorische gegevens \| Technische/diagnostische gegevens |
| **Gevoeligheid** | Normaal |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden \| Beheerder |

Gebruikers kunnen inloggen met hun gebruikersaccount of via single sign-on. De dienst implementeert Single Sign-On (SSO)-functionaliteit om gebruikersauthenticatie te stroomlijnen en te beveiligen. Gebruikers kunnen toegang krijgen tot de dienst via de native Salesforce-aanmeldingspagina, die Meervoudige Authenticatie (MFA) omvat, of via de eigen SSO-oplossing van hun instelling. De SSO-dienst wordt aangeboden door een partij die SSO implementeert op Salesforce. Instellingen maken rechtstreeks afspraken met deze partij. HR2day gebruikt cookies om te waarborgen dat de gebruiker gedurende de sessie ingelogd blijft.

De volgende cookies worden gebruikt voor authenticatie:

| Cookienaam | Leeftijd | Beschrijving |
|---|---|---|
| RSID | Sessie | Sessie-ID en log in als sessie-ID. Cookies gekopieerd naar respons en zorgen ervoor dat de doel-URL correct wordt opgebouwd in een proxysituatie. |
| SUCSP | Sessie | Gebruikt wanneer de gebruikersidentiteit die een beheerder aanneemt, via Log In als andere gebruiker, een gebruiker van de Customer Success Portal (CSP) is. |
| SUPRM | Sessie | Gebruikt wanneer de gebruikersidentiteit die een beheerder aanneemt, via Log In als andere gebruiker, een gebruiker van de Partner Relationship Management (PRM)-portal is. |
| sid | Sessie | Sessie-ID gebruikt om Lightning Platform Soap-API en Rest-API gegevensverbindingen te authenticeren voor de huidige gebruiker. |
| sid_Client | Sessie | Gebruikt om sessietampering te detecteren en voorkomen. |
| autocomplete | 60 dagen | Bepaalt of de aanmeldingspagina de gebruikersnaam van de gebruiker onthoudt. |
| disco | Sessie | Volgt de laatste gebruikersaanmelding en actieve sessie om aanmelding te omzeilen (bijv. OAuth immediate flow). |
| lloopch_loid | 1 jaar | Bepaalt of de gebruiker naar een specifieke portaalaanmelding of een app-aanmelding wordt gestuurd. |
| login | 60 dagen | Als de sessie van de gebruiker is verlopen, gebruikt om de gebruikersnaam op te halen en in te vullen op de hoofdaanmeldingspagina bij gebruik van de process builder-app. |

Tabel 4-1, cookies gebruikt bij aanmelden/afmelden.

### 4.3.2 Workflows

| | |
|---|---|
| **Doeleinden** | Medewerkerbeoordeling \| Medewerkeradministratie \| Ziekte- en verlofadministratie \| Salaris- en declaratieverwerking |
| **Gegevens** | Organisatorische gegevens \| Direct identificeerbaar \| Contactinformatie \| Demografische gegevens \| Communicatiegegevens \| Gezondheidsgegevens |
| **Gevoeligheid** | Normaal \| Gevoelig \| Bijzonder |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden \| Ex-medewerkers \| Partner / kind van (ex-)medewerker |

Instellingen kunnen hun eigen workflows ontwerpen in HR2day. Workflows zijn processen die bestaan uit een reeks stappen die automatisch op elkaar volgen. Ze bestaan om standaardtaken die elke keer dezelfde stappen volgen, gemakkelijker te maken. Voorbeelden zijn het indienen van verlofaanvragen, het melden van verzuim wegens ziekte, het indienen van declaraties en het doorgeven van wijzigingen in HR-gegevens, zoals adres, bankrekeningnummer, burgerlijke staat en competenties.

Deze stappen bestaan uit het indienen van wijzigingen door medewerkers/managers en kunnen ook een goedkeuring of afwijzing door een andere persoon omvatten. Elke afwijzing gaat vergezeld van een toelichting in een open tekstveld. Het invoeren van informatie in workflows is mogelijk via dropdown-menu's, meerkeuze-selectievakjes, vrije tekstvelden (lang of kort) en via het toevoegen van documenten. Verschillende rollen kunnen toegang hebben tot verschillende workflows, of verschillende stappen in verschillende workflows. Het aanmaken van en wijzigingen in bepaalde gegevens in de workflow worden ook gelogd (zie 4.3.10 Logging). Medewerkers en managers krijgen toegang tot verschillende workflows. Zo kunnen medewerkers verlofaanvragen indienen, zich ziek melden en wijzigingen in hun contactgegevens doorgeven, terwijl managers wijzigingen kunnen aanbrengen in de contracten en het salaris van hun medewerkers.

Medewerkers krijgen een overzicht van de lopende processen die ze zelf hebben geïnitieerd. Bovendien ontvangen ze notificaties voor acties die zij moeten ondernemen. Deze signalen kunnen ertoe leiden dat medewerkers een workflow moeten starten. Medewerkers krijgen geen overzicht van de workflows die betrekking op hen hebben en die hun managers hebben gestart.

Instellingen zijn vrij om hun eigen workflows te ontwerpen, maar in de standaardconfiguratie van HR2day zijn al enkele workflows aanwezig. Het is ook mogelijk om deze standaardworkflows te verwijderen.

### 4.3.3 Toegang tot persoonsgegevens via de EIC en MIC

| | |
|---|---|
| **Doeleinden** | Medewerkeradministratie \| Salaris- en declaratieverwerking \| Ziekte- en verlofadministratie |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Demografische gegevens \| Communicatiegegevens \| Gezondheidsgegevens \| Nationaal |

| | |
|---|---|
| | identificatienummer \| Raciale en/of etnische gegevens \| Gedragsgegevens \| Financiële gegevens |
| **Gevoeligheid** | Normaal \| Gevoelig |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden \| Ex-medewerkers |

In het Employee Interaction Centre kunnen medewerkers de volgende informatie raadplegen:

- Een overzicht van acties die de medewerker kan ondernemen, die workflows starten.
- Een overzicht van de afdelingskalender, waarop de afwezigheid van hun team zichtbaar is. Standaard maakt de kalender geen onderscheid tussen verzuim en verlof, maar werkgevers kunnen dit onderscheid zichtbaar maken.
- Hun salarisspecificaties. Het salaris is standaard verborgen en de medewerker moet erop klikken om het te zien.
- Een overzicht van notificaties, die ze kunnen uitschakelen.
- Een overzicht van hun verlof.
- Een overzicht van verzuim, anders dan verlof.
- Een grafiek van hun ontwikkeling.
- Een overzicht van openstaande acties, lopende processen en afgeronde processen.
- Het aantal openstaande declaraties en declaraties die worden verwerkt, met de optie om de declaraties zelf te tonen.
- Een overzicht van persoonlijke relaties.
- Een overzicht van koppelingen.
- Toegang tot hun documenten, die kunnen bevatten:
  - Kopie van identiteitspapieren
  - Salarisspecificaties
  - CV
  - Contracten
  - En andere documenten die zijn opgeslagen in het personeelsdossier

Het Manager Interaction Centre werkt op dezelfde manier, met twee verschillen:

- Omdat managers extra bevoegdheden hebben om gegevens van medewerkers in hun team in te zien, kunnen ze die informatie raadplegen in hun MIC (zie 4.3.9 Beheer van rollen en profielen).
- Managers hebben aanvullende toegang tot:
  - Verjaardagen.
  - Mogelijke rapportages die ze kunnen genereren.
  - De typen afwezigheid in de kalender voor leden van hun team.

### 4.3.4 Toegang tot en bewerken van het medewerkerdossier (direct)

| | |
|---|---|
| **Doeleinden** | Medewerkeradministratie \| Salaris- en declaratieverwerking \| Ziekte- en verlofadministratie |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Demografische gegevens \| Nationaal identificatienummer \| Communicatiegegevens \| Gezondheidsgegevens \| Gedragsgegevens \| Raciale en/of etnische gegevens \| Financiële gegevens |
| **Gevoeligheid** | Normaal \| Gevoelig \| Bijzonder |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden \| Ex-medewerkers |

Het tabblad 'Medew/HR gegevens', een afkorting voor medewerker-HR-gegevens, geeft (HR-)managers toegang tot volledige medewerkerdossiers. Naast het gebruik van workflows is het ook mogelijk om wijzigingen in dit dossier aan te brengen via workflows. Het bestaat uit:

- De basispersoonsgegevens van de medewerker
- Hun documenten
- Hun verzuim
- Hun verlof
- Hun (uitbetaalde) salarissen
- Hun persoonlijke relaties
- Hun beoordelingen
- Hun competenties en opleiding
- Hun arbeidsrelaties
- Hun declaraties
- Hun activiteiten en taken
- Hun digitale dossier
- Hun foto's en handtekeningen
- Hun geregistreerde gesprekken

Bij alle wijzigingen binnen workflows kunnen instellingen een vrij tekstveld toevoegen om de gebruiker de mogelijkheid te geven een toelichting bij de wijziging te geven. Er is ook de optie om een document toe te voegen.

*Zie 16.12 Verlies van controle door open tekstvelden.*

*Zie 16.13 Gebrek aan nauwkeurigheid door handmatige registratie van persoonsgegevens.*

### 4.3.5 Beheer van de arbeidsrelatie

| | |
|---|---|
| **Doeleinden** | Medewerkeradministratie \| Salaris- en declaratieverwerking |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Organisatorische gegevens \| Financiële gegevens |
| **Gevoeligheid** | Normaal \| Gevoelig |

| | |
|---|---|
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden \| Ex-medewerkers |

Het tabblad 'Medew/Arbeidsrelatie', een afkorting voor de arbeidsrelatie die de medewerker heeft met het bedrijf, stelt bepaalde gebruikers in staat het contract van de medewerker en verschillende salariscomponenten in te zien en te bewerken. De salariscomponenten zijn alle afzonderlijke elementen die het uiteindelijke salaris van een medewerker vormen, zoals basissalaris, bonussen, reiskostenvergoeding, etc. Op basis van deze componenten wordt het salaris van een medewerker berekend voor elke uitbetalingsperiode. Bevoegde gebruikers kunnen een volledig overzicht genereren van het salaris van de medewerker en alle elementen die zijn meegenomen bij de berekening daarvan, alsmede een loonstrook, die alleen de meest relevante informatie bevat. Instellingen kunnen bepalen wat er op de loonstrook wordt opgenomen.

Dit gedeelte van HR2day bevat ook de contractgegevens van de medewerker, zoals de startdatum, vakantiedagen en het rooster. Er zijn enkele vrije tekstvelden om de activiteiten van de medewerker en bijzondere details over de medewerker te registreren.

### 4.3.6 Documentbeheer

| | |
|---|---|
| **Doeleinden** | Medewerkeradministratie |
| **Gegevens** | Direct identificeerbaar \| Financieel \| Organisatorisch \| Demografisch \| Nationaal identificatienummer |
| **Gevoeligheid** | Normaal \| Gevoelig |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden \| Ex-medewerkers |

Alle documenten die in HR2day zijn aangemaakt en toegevoegd, worden opgeslagen in het digitale dossier, toegankelijk onder 'Medew/HR gegevens'. Dit omvat bestanden die zijn opgeslagen tijdens workflows en handmatig in het medewerkerdossier zijn geüpload, salarisspecificaties verzonden aan medewerkers en documenten die handmatig aan het dossier zijn toegevoegd. Er is een basisversie en een uitgebreide versie van het digitale dossierbeheer.

Met de uitgebreide versie kunnen gebruikers in documenten zoeken en vervaldatums instellen. Gebruikers kunnen een afwijkende vervaldatum instellen wanneer ze een bestand uploaden, die de centrale vervaldatum overschrijft. Het is ook mogelijk om gebruikers de toegang tot bepaalde documenten te blokkeren. Voor elk document worden de volgende gegevens geregistreerd:

- De maker van het document in HR2day
- De datum en het tijdstip van aanmaken
- De module waaronder het valt
- De categorie waaronder het valt
- De vervaldatum, indien aanwezig

Er is een standaardlijst met documentcategorieën, maar werkgevers kunnen ook hun eigen categorieën aanmaken. Gebruikers kunnen documenten vanuit HR2day per e-mail naar zichzelf verzenden.

#### 4.3.6.1 SignRequest

HR2day faciliteert het digitaal ondertekenen van documenten, voornamelijk arbeidscontracten maar ook andere HR-gerelateerde documenten, via SignRequest. Instellingen kunnen zelf bepalen welke documenten op deze manier worden ondertekend.

Een HR-manager bereidt een document voor binnen HR2day, dat vervolgens wordt verzonden naar SignRequest. SignRequest stuurt daarna een privélink naar de betrokkene via e-mail. Na het openen van de link moet de betrokkene de Servicevoorwaarden en het Privacybeleid van SignRequest accepteren voordat hij/zij het document kan bekijken en ondertekenen. Nadat het document is ondertekend, ontvangt de betrokkene een e-mailbevestiging en krijgt hij/zij de mogelijkheid om een kopie van het ondertekende document te downloaden voor zijn/haar administratie.

SignRequest gebruikt meerdere cookies en eindpunten om deze verwerking te faciliteren (zie Bijlage 1.3). HR2day heeft geen verdere informatie over SignRequest verstrekt. De reacties op de DSAR's (zie 3.2.1 Inzageverzoek betrokkenen) hebben ook geen duidelijkheid gegeven over deze verwerking.

Het merendeel van de eindpunten die tijdens onze technische analyse zijn gevonden voor SignRequest, bevindt zich buiten de EER (Europese Economische Ruimte). SURF heeft geen documentatie ontvangen over deze eindpunten en de cookies. Er is geen Data Transfer Impact Assessment (DTIA) met SURF gedeeld.

Tijdens het schrijven van deze DPIA is HR2day begonnen met het vervangen van SignRequest door ValidSign (eveneens een dochteronderneming van Visma).

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

#### 4.3.6.2 ValidSign

Tijdens het schrijven van deze DPIA was het systeem SignRequest gepland te worden uitgefaseerd ten gunste van het systeem ValidSign. Vanwege de timing van dit proces heeft ValidSign nog geen technische analyse ondergaan. Deze analyse wordt uitgevoerd tijdens de vervolgtest van het systeem. Er is echter al een juridische beoordeling van ValidSign uitgevoerd en de bevindingen zijn te vinden in 7.2.6 ValidSign.

### 4.3.7 Wijzigen en opslaan van gebruikersvoorkeuren

| | |
|---|---|
| **Doeleinden** | De dienst leveren en up-to-date houden \| De dienst personaliseren |
| **Gegevens** | Technische gegevens |
| **Gevoeligheid** | Normaal |

| | |
|---|---|
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden \| Beheerders |

Werkgevers kunnen een standaardinrichting selecteren voor de panelen van de EIC en de MIC, maar medewerkers kunnen de panelen ook zelf naar eigen voorkeur inrichten. Zij hebben ook de optie om notificaties individueel uit te schakelen.

Alle instellingen van de gebruikersinterface worden opgeslagen via cookies; zie Tabel 18-4 voor de lijst van cookies die HR2day gebruikt om voorkeuren op te slaan.

### 4.3.8 Genereren van rapporten

| | |
|---|---|
| **Doeleinden** | Interne rapportages |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Organisatorische gegevens \| Gezondheidsgegevens |
| **Gevoeligheid** | Normaal \| Gevoelig \| Bijzonder |
| **Betrokkenen** | Niet-bezoldigde personeelsleden \| Medewerkers \| Ex-medewerkers |

Het is mogelijk om rapporten, analyses en dashboards te genereren op basis van alle gegevens in HR2day. HR2day biedt een aantal standaardrapporten. Werkgevers kunnen ook hun eigen rapporten aanpassen en precies de (persoons)gegevens selecteren die ze willen opnemen. Gebruikers kunnen kiezen of ze de rapporten genereren in HR2day of in Excel-formaat.

### 4.3.9 Beheer van rollen en profielen

| | |
|---|---|
| **Doeleinden** | De dienst leveren en up-to-date houden \| De dienst beveiligen |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Organisatorische gegevens |
| **Gevoeligheid** | Normaal |
| **Betrokkenen** | Niet-bezoldigde personeelsleden \| Medewerkers \| Ex-medewerkers |

Het autorisatiemodel van HR2day is ontworpen om toegang tot gevoelige HR-gegevens op een gestructureerde manier te beheren en te controleren. Toegang is afgeleid van de organisatorische gegevens van gebruikers. Men begint zonder toegang. Dit Role Based Access Control-model bestaat uit meerdere lagen:

1. Profiel De toegang wordt bepaald door gebruikersprofielen, die definiëren welke acties (Aanmaken, Lezen, Bijwerken, Verwijderen) een gebruiker kan uitvoeren op elk type gegevens (object) op basis van hun functie (bijv. medewerker, manager, professional).

2. Organisatiebrede standaarden Organisatiebrede standaardinstellingen stellen het basisniveau van toegang vast voor alle gebruikers tot elk object.

3. Deelregels Deelregels kunnen handmatig worden aangemaakt of automatisch via op rollen gebaseerd delen.

3a. Handmatig delen & eigendom Toegang kan verder worden verfijnd door specifieke records handmatig te delen of op basis van wie eigenaar is van de gegevens. Deze optie wordt alleen

gebruikt wanneer andere opties niet toereikend zijn. Wanneer ze wordt gebruikt, is het altijd voor een zeer specifieke situatie, betreffende een zeer beperkt aantal gebruikers.

3b. Op rol gebaseerd delen Op rol gebaseerd delen is de standaard in HR2day. Rechten worden verleend op basis van organisatorische rollen, zodat gebruikers toegang hebben tot gegevens die relevant zijn voor hun verantwoordelijkheden.

De breedste toegang wordt verleend via deelregels, die op basis van gedefinieerde criteria toegang kunnen verlenen aan groepen gebruikers.

Kernpunten:

- Organisatiestructuur: Managers hebben standaard toegang tot de gegevens van medewerkers waarvoor zij verantwoordelijk zijn én van alle medewerkers die hiërarchisch onder deze medewerkers vallen. Hiërarchische overerving van toegangsrechten is standaard ingeschakeld.
- Functionele rol: Gebruikers kunnen toegang hebben tot gegevens die relevant zijn voor hun functionele rol (zoals verzuimbeheer, verlof, etc.).
- Functie: De toegang is afgestemd op de functie van de gebruiker.
- Bredere toegang: Naarmate men door de lagen heen gaat, wordt de toegang breder. Gebruikers krijgen toegang tot alle persoonsgegevens van alle medewerkers onder hen in de verticale lijn van de hiërarchie. Met de functionaliteit voor hiërarchische rechterovererving ingeschakeld, is het niet mogelijk deze toegang te beperken tot bepaalde typen persoonsgegevens, zodat een persoon alleen toegang heeft tot de typen persoonsgegevens die nodig zijn voor de uitvoering van zijn/haar taken.
- Conflictoplossing: Als deelregels conflicteren, geldt de meest permissieve regel.

### 4.3.10 Logging

| | |
|---|---|
| **Doeleinden** | Medewerkeradministratie \| De dienst beveiligen \| De dienst verbeteren \| De dienst leveren en up-to-date houden |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Organisatorische gegevens \| Communicatiegegevens \| Technische gegevens |
| **Gevoeligheid** | Normaal |
| **Betrokkenen** | Niet-bezoldigde personeelsleden \| Medewerkers \| Ex-medewerkers \| Beheerders |

HR2day gebruikt zes typen logging. Deze logging-opties worden aangeboden door Salesforce als onderdeel van de platformfunctionaliteit:

- Inloghistorie (login history)
- Actielog (event monitoring)
- Wijzigingshistorie (change history tracing)
- Foutlogs (error logging / foutopsporingslogboeken)
- Logboek van instellingswijzigingen (setup audit trail)

- E-maillogboek (email logs / emaillogboekbestanden)

HR2day heeft aangegeven dat dit alle logging is die zij uitvoeren. SURF heeft geen informatie over logging door hun subverwerkers anders dan Salesforce en Expo.

#### 4.3.10.1 Salesforce

Volgens HR2day heeft Salesforce waarschijnlijk een vorm van monitoringlogging voor beveiligingsdoeleinden, maar HR2day heeft hier geen toegang toe en heeft ook geen informatie over deze logging verstrekt.[23] SURF heeft verspreid door de documentatie van Salesforce informatie gevonden over logging. Er is echter geen duidelijk beeld van wat van toepassing is op de situatie van HR2day, omdat de documentatie van Salesforce betrekking heeft op meer of alle diensten.

Salesforce stelt in hun document 'The Salesforce Platform - Transformed for Tomorrow' dat zij gegevens verzamelen als een van hun architectuurprincipes:

> *"Integratie van alle diensten in een standaard observabiliteitsplatform voor efficiënte monitoring, waaronder het verzamelen van logs, het meten van statistieken, waarschuwingen, gedistribueerde tracering en het bijhouden van dienstbewerkingen zoals verkeersvolume, foutenpercentages en gebruik van hulpbronnen."*[24]

SURF heeft via de DSAR's geen informatie ontvangen over het verzamelen van loggegevens door Salesforce, en er is ook geen duidelijke documentatie over hoe Salesforce logging uitvoert voor eigen doeleinden. HR2day heeft een document verstrekt dat het onderscheid uitlegt dat Salesforce maakt tussen Klantgegevens (alle gegevens die door of namens klanten in de applicatie zijn ingevoerd, inclusief persoonsgegevens van medewerkers van de eindklanten van HR2day) en Gebruiksgegevens (gegevens gegenereerd door het gebruik van het platform, voor operationele, beveiligings- en analytische doeleinden). De meest gedetailleerde beschrijving van de Gebruiksgegevens die Salesforce verzamelt is:

> *"Salesforce kan het gebruik van de Covered Services volgen en analyseren voor beveiligingsdoeleinden en om Salesforce te helpen zowel de Covered Services als de gebruikerservaring bij het gebruik van de Covered Services te verbeteren. We kunnen deze informatie bijvoorbeeld gebruiken om trends te begrijpen en analyseren of bij te houden welke van onze functies het meest worden gebruikt om de productfunctionaliteit te verbeteren."*[25]

Eventuele identificerende informatie in de Gebruiksgegevens wordt geanonimiseerd voordat medewerkers van Salesforce er toegang toe krijgen.[26] Salesforce stelt daarom dat de Gebruiksgegevens worden verwerkt op een manier die het niet mogelijk maakt individuen te identificeren.[27] HR2day heeft de anonimiseringsmethoden die Salesforce gebruikt om de als Gebruiksgegevens verzamelde persoonsgegevens te anonimiseren, eventuele contractuele afspraken die Salesforce aan zijn toezeggingen binden, of een uitputtende lijst van specifieke gegevensvelden die Salesforce verzamelt niet verstrekt. SURF heeft daarom niet kunnen verifiëren dat Salesforce geen persoonsgegevens verwerkt bij het verzamelen van gebruiksgegevens.

[23] E-mail van HR2day, 15 mei 2025.
[24] The Salesforce Platform - Transformed for Tomorrow (https://architect.salesforce.com/fundamentals/platform-transformation)
[25] Hyperforce Security, Privacy and Architecture, https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/misc/hyperforce-security-privacy-and-architecture.pdf, p. 13, geraadpleegd op 23 januari 2026.
[26] E-mail van HR2day-contractant, ontvangen op 22 januari 2026.
[27] Uitleg van de verwerking van data door Salesforce door HR2day, ontvangen op 2 januari 2026.

#### 4.3.10.2 Inloghistorie

| | |
|---|---|
| **Doeleinden** | De dienst beveiligen |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Organisatorische gegevens \| Technische gegevens |
| **Gevoeligheid** | Normaal |
| **Betrokkenen** | Niet-bezoldigde personeelsleden \| Medewerkers \| Ex-medewerkers \| Beheerders |
| **Bewaartermijn** | 6 maanden |
| **Toegang** | Systeembeheerder |

Dit log toont details over de inloghistorie van gebruikers en wordt gebruikt voor het beveiligen van de dienst, zoals het monitoren van verdachte activiteiten. Het log kan worden ingezien en bekeken via de HR2day-interface en worden gedownload als .csv-bestand (door komma's gescheiden waarden).

**Inzageverzoek betrokkenen**

Alle gegevens die tijdens onze test in dit log zijn gegenereerd, waren opgenomen in de dataset die HR2day ons heeft verstrekt na onze indiening van een inzageverzoek.

#### 4.3.10.3 Actielog (Event monitoring)

| | |
|---|---|
| **Doeleinden** | De dienst beveiligen |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Organisatorische gegevens \| Technische gegevens |
| **Gevoeligheid** | Normaal |
| **Betrokkenen** | Niet-bezoldigde personeelsleden \| Medewerkers \| Ex-medewerkers \| Beheerders |
| **Bewaartermijn** | 3 dagen[28] |
| **Toegang** | Systeembeheerder |

Event logging is geïmplementeerd om zes typen gebeurtenissen bij te houden. Deze gebeurtenissen worden bijgehouden om de dienst te beveiligen. Eventlogs helpen verdachte activiteiten en mogelijke inbreuken te detecteren door gebruikersacties, aanmeldingen en

systeemgebeurtenissen te registreren, waardoor snelle identificatie en reactie op bedreigingen mogelijk wordt.

| Type event logging | Beschrijving |
|---|---|
| Login | Dit overzicht toont details over de inloghistorie van gebruikers en wordt gebruikt voor beveiligingsdoeleinden, zoals het monitoren van verdachte activiteiten. |
| Logout | Dit toont details van gebruikerssessies die worden beëindigd. Het doel is om beveiligingsmaatregelen te ondersteunen. |
| Hostname Redirects | Dit overzicht toont details van zowel geblokkeerde als geslaagde doorverwijzingen tijdens het inloggen. Doorverwijzingen kunnen optreden als gevolg van gewijzigde naamgeving; als deze niet zijn bijgewerkt in de code van HR2day of in de bladwijzers van gebruikers, kunnen gebruikers niet inloggen. Het detecteren hiervan maakt het mogelijk dit te verhelpen in de HR2day-code of door gebruikers te contacteren om hun bladwijzers bij te werken. |
| CSP Violation | Dit overzicht toont details van geblokkeerde verzoeken op Lightning Experience-pagina's. Het biedt inzicht in of er pogingen zijn tot hackaanvallen op HR2day binnen het Salesforce-platform. |
| API Total Usage | Geeft details over API-verzoeken. Het doel is inzicht te hebben in het gebruik van API's in een omgeving. |
| Apex Unexpected Exceptions | Rapporteert fouten in Apex-code in HR2day/Salesforce zodat deze kunnen worden opgelost en de software kan worden verbeterd. |

Tabel 4-2, de zes typen event logging.

De persoonsgegevens die worden verwerkt in deze typen event logging zijn te raadplegen in Tabel 18-9, verwerkte persoonsgegevens in event logging bij inloggen.

**Inzageverzoek betrokkenen**

Alle gegevens die tijdens onze test (3.2.1 Inzageverzoek betrokkenen) in deze logs zijn gegenereerd, waren NIET opgenomen in de dataset die HR2day ons heeft verstrekt na onze indiening van een inzageverzoek.

[28] Het Apex Unexpected Exceptions-log wordt voor onbepaalde tijd bewaard nadat de gegevens zijn geanonimiseerd. Zie 5.4.1 voor meer informatie over de anonimisering.

### 4.3.10.4 Wijzigingshistorie (Change History Tracing)

| | |
|---|---|
| **Doeleinden** | De dienst beveiligen |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Organisatorische gegevens \| Technische gegevens |
| **Gevoeligheid** | Normaal \| Gevoelig |

| | |
|---|---|
| **Betrokkenen** | Niet-bezoldigde personeelsleden \| Medewerkers \| Ex-medewerkers \| Beheerders |
| **Bewaartermijn** | 24 maanden |
| **Toegang** | Systeembeheerder |

Change History Tracing maakt het mogelijk te loggen wie welk veld heeft gewijzigd en wanneer, inclusief de vorige waarde. Het doel is de instelling (klant) te voorzien van bewijs voor interne controles en externe audits (bijv. accountants) om aan te tonen wie welke wijzigingen heeft aangebracht en wanneer.

Er geldt een limiet van maximaal 20 velden per object waarvoor change history tracing kan worden ingeschakeld. HR2day heeft standaard de volgende 17 objecten ingeschakeld:

- Afdeling
- Arbeidsrelatie
- Arbeidsrelatiewijziging
- Declaratiecategorie
- Declaratiecategorie Runtime
- Document Signflow Ondertekenaar
- Kostenplaats
- LooncompDefinitie
- Looncomponent
- Medew/HR gegevens
- Medew/HR gegevens wijziging
- MessageInfo
- Opleidingswijziging
- Review
- SignRequest[29]
- Werkgever

De instelling/klant kan via hun systeembeheerder wijzigen op welke velden change history tracing is ingeschakeld.

**Inzageverzoek betrokkenen**

Alle gegevens die tijdens onze test (3.2.1 Inzageverzoek betrokkenen) in dit log zijn gegenereerd, waren opgenomen in de dataset die HR2day ons heeft verstrekt na onze indiening van een inzageverzoek.

[29] Met de introductie van ValidSign als vervanging voor SignRequest zal dit veranderen.

### 4.3.10.5 Foutlogs (Debug Logs)

| | |
|---|---|
| **Doeleinden** | De dienst verbeteren \| De dienst leveren en up-to-date houden |

| | |
|---|---|
| **Gegevens** | Direct identificeerbaar \| Organisatorische gegevens \| Technische gegevens |
| **Gevoeligheid** | Normaal |
| **Betrokkenen** | Niet-bezoldigde personeelsleden \| Medewerkers \| Ex-medewerkers \| Beheerders |
| **Bewaartermijn** | 7 dagen |
| **Toegang** | Systeembeheerder |

Met foutlogs (debug logs) kan HR2day nagaan waar het fout gaat wanneer een gebruiker een foutmelding ontvangt. Het doel is deze fouten te verhelpen en daarmee het systeem te verbeteren. Voor een gebruiker is logging van zijn/haar transacties standaard uitgeschakeld. De foutlogs worden 7 dagen bewaard en worden daarna automatisch verwijderd door Salesforce.

Het log bevat de volgende velden per gebeurtenis:

- Uitvoereenheden
- Code-eenheden
- Logboekvermeldingen
- Tijdstempel
- Gebeurtenisindicator
- Cumulatief resourcegebruik
- Cumulatieve profileringsgegevens
- API-versie
- Logboekcategorie
- Logboekniveau

**Inzageverzoek betrokkenen**

Deze logregistratie was niet ingeschakeld in de testomgeving, waardoor er tijdens onze test geen gegevens in dit log zijn gegenereerd.

#### 4.3.10.6 Logboek van instellingswijzigingen (Setup Audit Trail)

| | |
|---|---|
| **Doeleinden** | De dienst beveiligen |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Organisatorische gegevens \| Technische gegevens |
| **Gevoeligheid** | Normaal \| Gevoelig |
| **Betrokkenen** | Beheerders |
| **Bewaartermijn** | 6 maanden |
| **Toegang** | Systeembeheerder |

Setup Audit Trail is een functie in Salesforce die automatisch alle configuratiewijzigingen registreert. Het houdt bij welke gebruiker welke wijzigingen heeft aangebracht en wanneer in de instellingen van uw Salesforce-omgeving. Deze logging wordt gebruikt om een auditspoor te hebben om ongeoorloofde wijzigingen in de systeeminstellingen te detecteren; het genereert ook een volledige geschiedenis van de systeemconfiguratie.

Het log bevat de volgende velden per gebeurtenis:

- Gebruiker
- Tijdstempel
- Type wijziging
- Details
- IP-adres
- Sessie-informatie
- Gebruiker die de wijziging heeft aangebracht
- Tijdstip van de wijziging
- Type wijziging (bijvoorbeeld: nieuw veld, workflow aangepast)
- Details van wat er precies is gewijzigd
- IP-adres van waaruit de wijziging is aangebracht
- Sessie-informatie

**Inzageverzoek betrokkenen**

Alle gegevens die tijdens onze test (3.2.1 Inzageverzoek betrokkenen) in dit log zijn gegenereerd, waren NIET opgenomen in de dataset die HR2day ons heeft verstrekt na onze indiening van een inzageverzoek.

#### 4.3.10.7 E-maillogboek (Email Logs)

| | |
|---|---|
| **Doeleinden** | De dienst beveiligen |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Organisatorische gegevens \| Technische gegevens |
| **Gevoeligheid** | Normaal \| Gevoelig |
| **Betrokkenen** | Niet-bezoldigde personeelsleden \| Medewerkers \| Ex-medewerkers \| Beheerders |
| **Bewaartermijn** | 30 dagen |
| **Toegang** | Systeembeheerder |

E-maillogboeken worden gebruikt om de status van e-mailbezorging te bepalen. Als het verzenden mislukt, is ook een foutcode beschikbaar die aangeeft waarom het verzenden is mislukt.

Bijlage 1.5 bevat een volledige lijst van de gegevens die worden verwerkt voor deze logging-activiteit.

**Inzageverzoek betrokkenen**

Alle gegevens die tijdens onze test (3.2.1 Inzageverzoek betrokkenen) in dit log zijn gegenereerd, waren NIET opgenomen in de dataset die HR2day ons heeft verstrekt na onze indiening van een inzageverzoek.

### 4.3.11 Fingerprinting en inbraakdetectie

| | |
|---|---|
| **Doeleinden** | De dienst beveiligen |
| **Gegevens** | Direct identificeerbaar \| Technische gegevens |
| **Gevoeligheid** | Normaal |
| **Betrokkenen** | Niet-bezoldigde personeelsleden \| Medewerkers \| Ex-medewerkers \| Beheerders |

HR2day en derde partijen verzamelen persoonsgegevens door cookies te plaatsen in de browsers van gebruikers. Zie bijlage 1.4 voor een volledige lijst van alle cookies en doeleinden.

- Fingerprinting
- Authenticeren
- Inbraakdetectie door Salesforce

HR2day gebruikt de volgende cookies voor beveiligingsdoeleinden; deze cookies worden gebruikt om een vingerafdruk (fingerprint) van de betrokkene te maken:

| Cookienaam | Leeftijd | Beschrijving |
|---|---|---|
| 79eb100099b9a8bf | Sessie | Browser Fingerprint trigger-cookie. Gebruikt om beveiligingsproblemen met sessies te detecteren. |
| 52609e00b7ee307e | Sessie | Browser Fingerprint-cookie. Gebruikt om beveiligingsproblemen met sessies te detecteren. |
| __Host-ERIC_PROD-<willekeurig getal> | 1 minuut | Enterprise Request Infrastructure Cookie (ERIC) draagt het CSRF-beveiligingstoken over tussen de server en de client. De naam geeft de servermodus aan (PROD/PRODDEBUG) en een willekeurig getal. Ander token voor elke Lightning-app. |
| __Host-ERIC_PRODDEBUG-<willekeurig getal> | | Enterprise Request Infrastructure Cookie (ERIC) draagt het CSRF-beveiligingstoken over tussen de server en de client. De naam geeft de servermodus aan (PROD/PRODDEBUG) en een willekeurig getal. Ander token voor elke Lightning-app. |
| clientSrc | Sessie | Gebruikt voor beveiligingsbescherming. |

Tabel 4-3, cookies gebruikt voor fingerprinting en/of inbraakdetectie.

## 4.4 Verstrekking

### 4.4.1 E-mailen

| | |
|---|---|
| **Doeleinden** | Medewerkeradministratie \| Interne rapportages |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Demografische gegevens \| Organisatorische gegevens \| Gezondheidsgegevens \| Financiële gegevens |
| **Gevoeligheid** | Normaal \| Gevoelig \| Bijzonder |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden \| Ex-medewerkers |

Gebruikers kunnen kopieën van documenten en Excel-versies van rapportages waartoe zij toegang hebben per e-mail naar zichzelf verzenden.

HR2day verstuurt ook een nieuwsbrief aan supergebruikers en andere gebruikers die zich hebben aangemeld.

### 4.4.2 Downloaden

| | |
|---|---|
| **Doeleinden** | Medewerkeradministratie \| Interne rapportages |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Demografische gegevens \| Organisatorische gegevens \| Gezondheidsgegevens \| Financiële gegevens |
| **Gevoeligheid** | Normaal \| Gevoelig \| Bijzonder |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden \| Ex-medewerkers |

Gebruikers kunnen documenten, rapporten en logboekoverzichten downloaden vanuit de gebruikersinterface van HR2day.

### 4.4.3 Ontvangen van notificaties

| | |
|---|---|
| **Doeleinden** | De dienst personaliseren \| Medewerkeradministratie |
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Organisatorische gegevens \| Demografische gegevens |
| **Gevoeligheid** | Normaal |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden |

De HR2day+ App kan notificaties ontvangen; dit zijn meldingen over bepaalde wijzigingen of signalen. HR2day gebruikt een geautomatiseerd notificatiemechanisme dat medewerkers en managers informeert over activiteiten die aandacht vereisen.

Medewerkers ontvangen notificaties voor nieuw beschikbare documenten (zoals loonstroken en jaaropgaven), goedkeuringen of afwijzingen van verlofaanvragen, ingediende declaraties en statusupdates, beslissingen over procesbeheer (goedkeuring/afwijzing) en algemene systeemmededeling.

Managers ontvangen notificaties over openstaande verlofaanvragen, algemene wijzigingen die wachten op goedkeuring, ingediende declaraties en professionaliseringsaanvragen van hun teamleden.

Elke notificatie heeft een vooraf ingestelde titel, bijvoorbeeld: "Een nieuwe loonstrook is beschikbaar" of "Een nieuwe jaaropgave is beschikbaar". Deze notificaties bevatten doorgaans een notificatietekst met persoonsgegevenselementen zoals de naam van de medewerker, relevante datums (begin-/einddatum verlof), documentidentificatoren (declaratienummers), goedkeuringsstatus en redenen voor afwijzing. Bestandsnamen van documenten kunnen persoonlijke informatie onthullen.

Notificaties zijn standaard ingeschakeld en gebruikers kunnen de notificatievoorkeuren individueel beheren, omdat de app de gebruiker vraagt of hij/zij notificaties wil ontvangen. Er is geen gedetailleerde controle voor gebruikers om te definiëren welke notificaties ze wel of niet willen ontvangen.

De gedetailleerde specificaties van alle notificatietypen, triggeringsomstandigheden en verzonden gegevenselementen zijn gedocumenteerd in Bijlage 0 HR2day App Push Notifications.

De app gebruikt Expo als subverwerker voor de verwerking van deze notificaties. Notificaties worden verzonden via de pushnotificatieservice van Expo, waarvoor de app het apparaat moet registreren en een uniek token voor elk apparaat moet verkrijgen.

Expo verwijdert de payload van de pushmelding nadat deze is gedeeld met Google of Apple.[30] Notificaties worden alleen opgeslagen in het geheugen en in berichtenwachtrijen, niet in databases.

Expo zelf is een cloudservice gevestigd in de VS, en gegevens kunnen worden verwerkt in verschillende datacenters, afhankelijk van de servicearchitectuur en de locatie van de gebruikers.

De metadata die door Expo worden opgeslagen, in dit geval:

- Pushtokens: dit zijn persistente identificatoren die verwijzen naar individuele apparaten en die moeten worden bewaard om de dienst te laten functioneren.
- Pushrapporten: registratie van welke notificaties succesvol zijn bezorgd bij Google/Apple.
- Auditlogs: registraties van bezorgingspogingen en -status.
- Apparaatinformatie van de gebruiker, crashtracering en IP-adres.

De metadata wordt verwerkt voor de duur van de overeenkomst, of zoals anderszins vereist door de wet of overeengekomen tussen de partijen.[31] Expo gebruikt apparaatinformatie van gebruikers voor geaggregeerde trendanalyse.[32]

[30] EXPO FAQ – https://docs.expo.dev/push-notifications/faq/

[31] Verwerkersovereenkomst Expo en HR2day – Expo DPA – 2025.pdf

[32] Verwerkersovereenkomst Expo en HR2day – Expo DPA – 2025.pdf

### 4.4.4 Verwerken van ondersteuningsverzoeken

| | |
|---|---|
| **Doeleinden** | Klantenondersteuning bieden |

| | |
|---|---|
| **Gegevens** | Direct identificeerbaar \| Contactinformatie \| Communicatiegegevens \| Organisatorisch |
| **Gevoeligheid** | Normaal |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden \| Ex-medewerkers |

Alleen supergebruikers kunnen ondersteuningsverzoeken indienen via tickets in het 'Klantportaal'. In sommige uitzonderlijke gevallen bellen of e-mailen zij ook HR2day. In het Klantportaal kunnen zij het volgende invoeren:

- Onderwerp van het verzoek
- Beschrijving van het verzoek in een vrij tekstveld
- Bijlage

### 4.4.5 Proxy-login (inloggen als)

| | |
|---|---|
| **Doeleinden** | Klantenondersteuning bieden |
| **Gegevens** | Direct identificeerbaar \| Contactgegevens \| Demografische gegevens \| Communicatiegegevens \| Organisatorische gegevens \| Gezondheidsgegevens \| Financiële gegevens \| Vakbondsgegevens \| Politieke gegevens |
| **Gevoeligheid** | Normaal \| Gevoelig \| Bijzonder |
| **Betrokkenen** | Medewerkers \| Niet-bezoldigde personeelsleden \| Ex-medewerkers |

HR2day biedt functionaliteit die wordt aangeduid als 'inloggen als / login as access', waarmee bevoegde beheerders van de verwerkingsverantwoordelijke tijdelijk de identiteit van een andere gebruiker binnen het systeem kunnen aannemen. Wanneer deze modus is ingeschakeld, ervaart de beheerder het systeem precies zoals de gebruiker wiens identiteit wordt aangenomen dat zou doen, inclusief volledige toegang tot diens interface, rechten en persoonsgegevens.

Het inschakelen van deze functionaliteit is naar eigen inzicht van de instelling, en HR2day dwingt deze functie niet af en configureert deze ook niet standaard. De functie omvat slechts beperkte logging. Er wordt geregistreerd wanneer een beheerder een sessie waarin hij zich voordoet als een andere gebruiker start en beëindigt (4.3.10.6 Logboek van instellingswijzigingen), maar acties die tijdens die sessie worden uitgevoerd, worden gelogd alsof ze door de gebruiker zijn uitgevoerd in wiens naam de beheerder optreedt (4.3.10.4 Wijzigingshistorie). Weergave- of alleen-lezen-activiteiten worden niet gelogd.

# 5 Technieken en methoden van verwerking

## 5.1 Zoeken

De zoekfunctionaliteit in HR2day maakt gebruik van Einstein Search, een AI-oplossing op het Lightning-platform.[33] Hiermee kunnen gebruikers:

- "Gepersonaliseerde resultaten ontvangen op basis van hoe u in Salesforce werkt.
- Direct voorgestelde records en previews zien wanneer u begint te typen.
- Een term invoeren en een aanbevolen resultaat ontvangen.
- Gewone woorden en zinnen gebruiken in de zoekbalk en relevante informatie ontvangen."[34]

Voor bepaalde functies van Einstein Search wordt gebruik gemaakt van:

- Klantgegevens en Salesforce-objecten, en/of
- Gebruiksgegevens.

Deze gegevens kunnen worden verwerkt in en worden gebruikt om globale modellen te trainen. Globale modellen zijn voorspellende modellen die worden getraind met gegevens van meerdere klantorganisaties van Salesforce.[35] Het is mogelijk om geen trainingsgegevens te leveren aan de globale modellen, terwijl de Einstein Search-functionaliteit toch beschikbaar blijft.

| Product | Functie | Klantgegevens en Salesforce-objecten gebruikt | Gebruiksgegevens gebruikt | Globaal model |
|---|---|---|---|---|
| Einstein Search | Einstein AI-gegenereerde zoek antwoorden | Kennis | Kenniszoektermen, kenniszoekresultaten (record-ID's, query en documentmatchmetadata), en kennisartikelmetadata. | Nee |
| Einstein Search | Einstein search | Nb | Zoektermen, zoekresultaten (record-ID's, query en documentmatchmetadata, en gebruikers-MRU en documentmatchmetadata), en org-metadata.<br>Zie How Does Einstein Search Use My Data. | Ja |
| Einstein Search voor Knowledge | Einstein search voor kennis | Nb | Kenniszoektermen, kenniszoekresultaten (record-ID's,<br>query en documentmatchmetadata, en gebruikers-MRU en | Ja |

| Product | Functie | Klantgegevens en Salesforce-objecten gebruikt | Gebruiksgegevens gebruikt | Globaal model |
|---|---|---|---|---|
| | | | documentmatchmetadata), en kennisartikelmetadata.<br>Zie Enable Einstein Search for Knowledge. | |

Een zoekquery was geen onderdeel van de testscenario's die in HR2day zijn uitgevoerd, waardoor Einstein Search buiten de technische testscope valt. SURF gaat ervan uit dat instellingen kiezen voor de opt-out voor het leveren van trainingsgegevens aan globale modellen.

[33] Natural Language Search Examples, https://help.salesforce.com/s/articleView?id=ai.search_ai_natural_lang_examples.htm&type=5, geraadpleegd op 7 mei 2026.

[34] Explore Einstein Search, https://help.salesforce.com/s/articleView?id=ai.search_ai_enduser_intro.htm&type=5, geraadpleegd op 7 mei 2026.

[35] Salesforce Einstein: Global Model Opt-Out Process, https://help.salesforce.com/s/articleView?id=000384050&type=1, geraadpleegd op 7 mei 2026.

## 5.2 API

HR2day maakt gebruik van de Salesforce REST API om hun Salesforce-instantie programmatisch te verbinden met andere interne of externe systemen. De REST API biedt een interface voor toegang tot vrijwel alles wat via de native gebruikersinterface kan worden gedaan. Klanten sturen verzoeken naar specifieke resource-URI's om gegevens, metadata en andere bronnen binnen de applicatie te raadplegen, te manipuleren, te doorzoeken en op te vragen.

Dit Salesforce Integration Platform gebruikt MuleSoft om het beheer van geautomatiseerde processen te faciliteren, waardoor een naadloze gegevensstroom en connectiviteit tussen Salesforce en aangepaste diensten of diensten van derden wordt gewaarborgd. Dit zorgt voor universele connectiviteitsondersteuning voor standaard API-specificaties zoals OpenAPI voor synchrone en AsyncAPI voor asynchrone interacties.

Klanten (HR2day of instellingen?) kunnen resources zoals de Portability-resource via de REST API gebruiken om persoonlijk identificeerbare informatie (PII) van klanten over records samen te stellen en te localiseren voor verzoeken om gegevensoverdraagbaarheid.

In de Salesforce API-documentatie[36] en in de documentatie van The Salesforce Platform[37] is gespecificeerd dat de zichtbaarheid van gegevens gebruikersspecifiek is. De gegevens die via de API kunnen worden geraadpleegd of bewerkt, zijn onderworpen aan dezelfde beveiligings- en deelcontroles die voor die gebruiker binnen HR2day van toepassing zijn.

[36] Salesforce REST API Developer Guide, Version 63.0, Spring '25.

[37] The Salesforce Platform - Transformed for Tomorrow | Salesforce Architects (https://architect.salesforce.com/fundamentals/platform-transformation).

## 5.3 Cookies

Cookies zijn kleine tekstbestanden die op een apparaat worden geplaatst bij een bezoek aan HR2day; deze cookies worden gebruikt om (persoons)gegevens op te slaan op het apparaat van de gebruiker.

Cookies in een dienst zoals HR2day kunnen worden gebruikt om:

- veilige gebruikerssessies te onderhouden
- gebruikersvoorkeuren en instellingen te onthouden bij volgende bezoeken
- naadloze authenticatie en autorisatie mogelijk te maken
- analyses te verzamelen voor verbetering van de dienst
- gebruikersconsent te verkrijgen en te beheren
- analyses te verzamelen voor verbetering van de dienst

HR2day gebruikt cookies om zijn diensten te ondersteunen: 6 cookies van HR2day, 33 cookies van Salesforce, 6 cookies van SignRequest en 1 cookie van een onbekende derde partij (MyFonts.net).

De cookieverklaring[38] die door HR2day is verstrekt, was alleen van toepassing op de publieke/commerciële website.

De cookieverklaring van HR2day documenteerde geen cookies die door hun SaaS-applicatie worden gebruikt.

De documentatie van de cookies die door HR2day worden geplaatst[39] werd op verzoek verstrekt door het technisch personeel van HR2day.

Op verzoek was HR2day in staat documentatie te produceren van een selectie van cookies die door Salesforce worden geplaatst.[40]

Om de volledige documentatie te verkrijgen van alle cookies die door Salesforce worden geplaatst, moest HR2day een ondersteuningsverzoek indienen bij Salesforce. De documentatie van de resterende cookies werd na contact met Salesforce-ondersteuning door HR2day-medewerkers verstrekt.

Alle cookies die door HR2day worden gebruikt, zijn functionele (vereiste) cookies en er is derhalve geen toestemmingsmechanisme (cookiebanner) aanwezig.

ValidSign is na onze technische analyse geïntroduceerd als vervanging voor SignRequest. Hierdoor zijn de door ValidSign gebruikte cookies niet opgenomen in deze beoordeling.

Raadpleeg Bijlage 1.4 Cookies voor een volledige lijst van gebruikte cookies.

Zie voor meer informatie 16.4 Verlies van controle door gebrek aan transparantie over de verwerking van persoonsgegevens via cookies.

[38] https://www.hr2day.com/cookie-statement/ – Cookieverklaring – HR2day.pdf.

[39] Raadpleeg Bijlage 1.4 Cookies voor een volledige lijst van gebruikte cookies.

[40] Cookiedocumentatie gepubliceerd op Salesforce Help – https://help.salesforce.com/s/articleView?id=xcloud.platform_cookies.htm&type=5

## 5.4 Anonimisering

Volgens de documentatie van The Salesforce Platform[41] worden logs geanonimiseerd, maar er wordt niet gespecificeerd welke gegevens worden gelogd en hoe de anonimisering plaatsvindt. Dit sluit aan bij onze bevindingen in paragraaf 4.3.10.1 Salesforce.

[41] The Salesforce Platform - Transformed for Tomorrow | Salesforce Architects (https://architect.salesforce.com/fundamentals/platform-transformation).

### 5.4.1 Apex Unexpected Exceptions Logging

De Apex Unexpected Exceptions Logging-gegevens worden anoniem opgeslagen. Dit wordt gedaan door de gebruikersgegevens uit de logs te verwijderen. De velden USER_ID en USER_ID_DERIVED worden uit deze dataset verwijderd.

## 5.5 Pseudonimisering

Er is geen documentatie over pseudonimisering verstrekt en HR2day heeft aangegeven dat zij deze functionaliteit niet hebben.[42]

[42] Communicatie HR2day, 10 juli 2025.

## 5.6 Testomgeving

HR2day biedt een functie in de testomgeving van HR2day om nep-medewerkers aan te maken, zodat tests en het accepteren van wijzigingen in het systeem kunnen worden uitgevoerd zonder gebruik van persoonsgegevens en zonder dat onnodige duplicaten hoeven te worden aangemaakt.

## 5.7 Gegevensencryptie

HR2day steunt op Salesforce voor beveiliging en is daarmee ook de aanbieder van de encryptiedienst. Salesforce hanteert een Zero-Trust Security-principe waarbij encryptie van gegevens zowel in transit als at rest is geïmplementeerd als onderdeel van hun verdedigingsstrategie.

#### Gegevens in transit

Salesforce gebruikt industrie-geaccepteerde end-to-end encryptieproducten om Klantgegevens en communicatie te beschermen tijdens de overdracht tussen het netwerk van een klant en de Salesforce-diensten, evenals binnen de Salesforce-infrastructuurdomeinen via Transport Layer Encryption (TLS).[43] Salesforce vereist TLS 1.2 als minimumprotocolversie voor zijn kerndiensten; nieuwere diensten en regio's ondersteunen in toenemende mate ook TLS 1.3. TLS 1.2+ wordt afgedwongen voor zowel externe clientverbindingen als door Salesforce

geïnitieerde verbindingen (API's, callouts, etc.). Oudere protocollen zoals TLS 1.0/1.1 worden niet meer ondersteund.

[43] Salesforce Services and Marketing Cloud Supported TLS Cipher Suites – https://help.salesforce.com/s/articleView?id=000380977&type=1 – geraadpleegd op 20-01-2026

### Gegevens at rest

HR2day heeft het C5 ISAE-rapport over Hyperforce gedeeld, dat stelt dat Salesforce de gegevens at rest versleutelt. Hyperforce maakt gebruik van AWS-opslagbronnen die standaard geconfigureerd zijn met ingeschakelde encryptie, waarbij gebruik wordt gemaakt van door de klant beheerde sleutels (CMK) via AWS Key Management Services (KMS). Salesforce beheert deze sleutels namens HR2day, inclusief het jaarlijkse rotatieproces.

Salesforce biedt aanvullende encryptieopties via zijn Salesforce Shield[44]-dienst, die specifiek is ontworpen om extra bescherming toe te voegen voor gevoelige gegevens en bijzondere categorieën persoonsgegevens. HR2day maakt echter geen gebruik van deze verbeterde encryptieniveaus. Als gevolg hiervan zijn gevoelige en bijzondere categorieën gegevens niet beschermd met cel-niveau encryptie.

[44] Salesforce Shield – https://www.salesforce.com/platform/shield/

### AWS[45]

De Klantgegevens zijn ook versleuteld at rest. Ten behoeve van het voorkomen van fraude of misbruik en om te voldoen aan toepasselijk recht, behoudt hostingprovider AWS de mogelijkheid om toegang te verkrijgen tot systemen die versleutelde Klantgegevens verwerken en opslaan.

Salesforce heeft technische maatregelen getroffen die verhinderen dat AWS toegang heeft tot onversleutelde Klantgegevens en tot de encryptiesleutels die worden gebruikt om Klantgegevens te versleutelen. Met Platform Encryption kunnen klanten encryptiesleutelmateriaal genereren en opslaan buiten Salesforce.

[45] C5 ISAE Report on Hyperforce – C5 ISAE Report – c5-isae-3000-report-salesforce-services-on-hyperforce_2024-11-01-2025-04-30.pdf

## 5.8 Back-up

Back-upbeleid en -procedures zijn gedocumenteerd en gecommuniceerd conform C5-controle SP-01, waarbij duidelijke vereisten worden gesteld voor de frequentie van gegevensback-ups en hersteldoelstellingen, met een Recovery Time Objective van 12 uur en een Recovery Point Objective van 4 uur.[46] Back-upgegevens worden bewaard in versleutelde vorm met behulp van encryptiestandaarden. Toegang tot back-upgegevens en het uitvoeren van herstelоperaties is beperkt tot bevoegd personeel. Salesforce beheert de encryptiesleutels.

Herstelprocedures worden regelmatig getest en gevalideerd om de integriteit en herstelbaarheid van back-upsystemen te waarborgen.

De gedeelde documentatie specificeert niet welke encryptiemethode door Salesforce wordt gebruikt voor gegevens at rest op Hyperforce, anders dan dat het state-of-the-art is. Volgens het C5 ISAE-rapport zijn er geen afwijkingen op de bijbehorende controles.

[46] Disaster Recovery Testing Summary Salesforce Hyperforce Infrastructure – February 2024 / January 2025 – geraadpleegd op 20-01-2026

# 6 Juridisch en beleidskader

## 6.1 Algemeen contractueel kader

HR2day verwerft de meeste klanten via aanbestedingen. Elke instelling bepaalt haar eigen, individuele eisen voor het product en de contracten die de leverancier moet accepteren. Dit betekent dat HR2day voor elke klant enigszins afwijkende contracten heeft. Op basis van een steekproef van contracten voor verschillende klanten, de vereisten voor een werkend contractueel kader en de rol van HR2day als verwerker, gaat deze DPIA ervan uit dat elke klant van HR2day ten minste een dienstverleningsovereenkomst (inclusief een beschrijving van de aanbestede diensten, indien van toepassing), een service level agreement en een verwerkersovereenkomst heeft op basis van:

- SURF Model Verwerkersovereenkomst SURF Juridisch Normenkader (Cloud)services 3.0[47], of
- SURF Model Verwerkersovereenkomst 4.0[48]

HR2day heeft ook algemene voorwaarden die van toepassing zijn op het gebruik van hun product. De toepasselijkheid hiervan is echter in de contracten uit de steekproef uitgesloten en vervangen door de ARBIT-voorwaarden. HR2day heeft bevestigd dat dit voor alle SURF-leden het geval is.

Zoals vermeld heeft HR2day voor elke klant een verwerkersovereenkomst, waarin zij zich verplicht de persoonsgegevens in HR2day uitsluitend te verwerken zoals noodzakelijk voor het leveren van de diensten zoals beschreven in de dienstverleningsovereenkomst, en deze gegevens niet voor eigen doeleinden te verwerken.[49] De voornaamste genoemde doeleinden zijn personeelsadministratie en salarisadministratie.

[47] https://www.surf.nl/files/2019-04/SURF-Model-Verwerkersovereenkomst-3.0.pdf, geraadpleegd op 14 mei 2025.

[48] https://www.surf.nl/surf-juridisch-normenkader-cloudservices, geraadpleegd op 14 mei 2025.

[49] Art. 2.3 Template Verwerkersovereenkomst HR2day.pdf

## 6.2 Toepasselijke wet- en regelgeving

Deze paragraaf bevat een niet-limitatieve lijst van wet- en regelgeving die van toepassing kan zijn op de verwerkingsactiviteiten die plaatsvinden in HR2day:

| Afkorting | Wet- of regelgevingskader | Relevante artikelen | Relevantie voor gebruikers HR2day (optioneel) |
|---|---|---|---|
| AWR | Algemene Wet inzake Rijksbelastingen | Art. 52(4) | Bewaartermijn voor bepaalde belastinggegevens |
| | Arbeidsomstandighedenbesluit | Diverse artikelen | HRM-wetgeving |
| Arbowet | Arbeidsomstandighedenwet | Art. 3 en 18 | HRM-wetgeving |
| | Arbeidstijdenwet | | HRM-wetgeving |
| AW | Archiefwet 1995, inclusief Archiefbesluit 1995 en Archiefregeling | Art. 5 | Wettelijke basis selectielijsten |
| | Selectielijsten hogescholen/universiteiten/mbo-instellingen | N.v.t. | Bewaartermijnen voor gegevens die onder de AW vallen |
| | Beleidsregels verwerking persoonsgegevens gezondheid zieke werknemers | N.v.t. | Regels voor de verwerking van persoonsgegevens over zieke werknemers |
| BW | Burgerlijk Wetboek Boek 7 | Art. 7:611 en art. 7:400 e.v. | Regels voor gedrag tussen medewerkers en werkgevers |
| | Informatiebeveiligingsbeleid | N.v.t. | Beleid inzake beveiligingspraktijken |
| | Privacybeleid van de instelling | N.v.t. | Beleid inzake privacypraktijken |
| Tw | Telecommunicatiewet | Diverse artikelen | Regels voor cookies en vergelijkbare technologieën |
| | Uitvoeringsregeling loonbelasting 2011 | Art. 7.5(4) en 12.1(5) | Identificatieplicht en bewaartermijn loonbelastingverklaring |
| UAVG | Uitvoeringswet AVG | Diverse artikelen | Nederlandse implementatie van de AVG |
| Wabb | Wet algemene bepalingen burgerservicenummer | Artikelen 10, 11, 12 en 13 | Regels voor de verwerking van nationale identificatienummers |
| Wfsv | Wet financiering sociale verzekeringen | Diverse artikelen | Regels inzake nationale verzekeringen |
| | Wet op de loonbelasting 1964 | Art. 28 | Belastingregels |
| WOR | Wet op de ondernemingsraden | Art. 27(1) | Regels inzake rechten van ondernemingsraden |

| Afkorting | Wet- of regelgevingskader | Relevante artikelen | Relevantie voor gebruikers HR2day (optioneel) |
|---|---|---|---|
| Wvp | Wet verbetering poortwachter | Diverse artikelen | Regels inzake langdurig ziekteverzuim |

# 7 Betrokken partijen

In dit hoofdstuk worden de verschillende partijen beschreven die betrokken zijn bij de gegevensverwerking in HR2day en hun rollen.

De AVG bevat definities van de verschillende rollen van bij de gegevensverwerking betrokken partijen: (gezamenlijke) verwerkingsverantwoordelijke, verwerker en subverwerker. Artikel 4 lid 7 AVG definieert de (gezamenlijke) verwerkingsverantwoordelijke als:

> *"een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen."*

Artikel 26 AVG bepaalt dat wanneer twee of meer verwerkingsverantwoordelijken gezamenlijk de doeleinden en middelen voor de verwerking bepalen, zij gezamenlijke verwerkingsverantwoordelijken zijn. Gezamenlijke verwerkingsverantwoordelijken moeten op transparante wijze, met name ten aanzien van betrokkenen, hun respectievelijke verantwoordelijkheden voor de nakoming van de AVG-verplichtingen vastleggen in een onderlinge regeling.

Artikel 4 lid 8 AVG definieert een verwerker als:

> *"een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt."*

Een subverwerker is een andere verwerker die door een verwerker wordt ingeschakeld en die bijdraagt aan de verwerking van persoonsgegevens namens een verwerkingsverantwoordelijke.

Artikel 28 AVG bevat diverse verplichtingen van verwerkers jegens de verwerkingsverantwoordelijken voor wie zij gegevens verwerken. Artikel 28 lid 3 AVG bevat specifieke verplichtingen voor de verwerker. Tot deze verplichtingen behoort het uitsluitend verwerken van persoonsgegevens op grond van gedocumenteerde instructies van de verwerkingsverantwoordelijke en het meewerken aan audits door een verwerkingsverantwoordelijke. Artikel 28 lid 4 AVG bepaalt dat een verwerker voor het uitvoeren van specifieke verwerkingstaken subverwerkers mag inschakelen, maar alleen met voorafgaande toestemming van de verwerkingsverantwoordelijke.

Bij de beoordeling van rollen in het kader van gegevensbescherming is de formele contractuele rolverdeling niet leidend en niet doorslaggevend. De feitelijke rol van een partij dient primair te worden bepaald op basis van de feitelijke omstandigheden. SURF houdt dan ook rekening met deze omstandigheden bij het vaststellen van de rollen inzake gegevensbescherming in DPIA's.

## 7.1 Instellingen als verwerkingsverantwoordelijke en HR2day als verwerker

HR2day heeft verwerkersovereenkomsten met al haar klanten, waaruit blijkt dat de instellingen als klanten verwerkingsverantwoordelijke zijn voor de verwerkingsactiviteiten zoals beschreven in de verwerkersovereenkomsten (zie 2 Doeleinden). Omdat instellingen de doeleinden en middelen bepalen voor alle persoonsgegevens die zij in HR2day invoeren en verwerken in het kader van hun salaris- en personeelsadministratie, zijn zij verwerkingsverantwoordelijke voor deze verwerkingen. De verwerkingsactiviteiten zijn beschreven in hoofdstuk 4. Sommige verwerkingsactiviteiten vormen gegevensdoorgiften, die worden beschreven in hoofdstuk 9. HR2day is verwerker voor de verwerkingsactiviteiten die zijn beschreven in de verwerkersovereenkomsten.

## 7.2 Subverwerkers

De in de verwerkersovereenkomst van HR2day genoemde subverwerkers zijn:

| Naam | Verwerkingsactiviteiten | Persoonsgegevens |
|---|---|---|
| Salesforce | Salesforce beheert, onderhoudt en ontwikkelt het platform (force.com) waarop HR2day is ontwikkeld en beschikbaar wordt gesteld. | Alle persoonsgegevens die worden verwerkt in en via HR2day |
| SignRequest | SignRequest is een aanbieder van de oplossing voor het elektronisch ondertekenen van overeenkomsten. | Gegevens digitale handtekening |
| Workbee | Workbee is de 'makelaar' die ervoor zorgt dat de (verzuim)gegevens vanuit HR2day worden doorgezonden naar de arbodienst van de verwerkingsverantwoordelijke. | Verzuimgegevens |
| Infor | Infor is de leverancier van de HR Analytics-oplossing waarin persoonsgegevens ook worden opgeslagen voor rapportagedoeleinden. | Alle persoonsgegevens in de HR2day-applicatie |

Uit het technisch onderzoek en de gesprekken met de leverancier bleek bovendien dat HR2day nog twee subverwerkers gebruikt die niet zijn vermeld in de verwerkersovereenkomsten met de instellingen.

| Naam | Verwerkingsactiviteiten | Persoonsgegevens |
|---|---|---|
| Expo | Expo maakt het verzenden van notificaties in de mobiele HR2day+ App mogelijk. | Onbekend |

| Naam | Verwerkingsactiviteiten | Persoonsgegevens |
|---|---|---|
| ValidSign | ValidSign is een aanbieder van de oplossing voor het elektronisch ondertekenen van overeenkomsten. | Gegevens digitale handtekening |

### 7.2.1 Salesforce

Salesforce levert het force.com-platform waarop de HR2day-applicatie draait. HR2day heeft een Platform Solution Reseller Agreement (PSRA) met Salesforce Inc., waarbij HR2day de Reseller is. Salesforce Inc. is gevestigd in San Francisco, in de Verenigde Staten. De generieke Salesforce Data Processing Addendum is bij deze overeenkomst gevoegd en is van toepassing op de gegevensverwerking die Salesforce als subverwerker uitvoert. Na een wijziging van de PSRA is de DPA met revisiедatum 2023 de van toepassing zijnde versie.[50] Deze verwerkersovereenkomst is alleen van toepassing op Klantgegevens (Customer Data), die Salesforce als volgt definieert:

> *"…alle elektronische gegevens of informatie die door een Klant zijn ingediend bij de systemen van SFDC en die voor de Klant toegankelijk zijn via de Gecombineerde Oplossing terwijl deze zich op de systemen van SFDC bevindt."*[51]

HR2day heeft Salesforce geen aanvullende contractuele instructies gegeven over de verwerking van persoonsgegevens en in de DPA zijn bepalingen opgenomen over het verwerken door Salesforce van persoonsgegevens die onder de DPA vallen voor eigen doeleinden. Volgens Salesforce heeft het bedrijf geen inzicht in de inhoud van Klantgegevens.[52]

Salesforce verwerkt persoonsgegevens:

> *"…uitsluitend namens Reseller en in overeenstemming met de gedocumenteerde instructies van Reseller (inclusief die welke namens de betreffende Klant worden overgebracht) en/of de instructies van een Klant, al naar gelang het geval, voor de volgende doeleinden: (i) Verwerking in overeenstemming met de Overeenkomst en toepasselijke Bestelbonnen; (ii) Verwerking geïnitieerd door Gebruikers bij hun gebruik van de Diensten; en (iii) Verwerking om te voldoen aan andere gedocumenteerde redelijke instructies van Reseller (inclusief die welke door of namens de betreffende Klant worden overgebracht (bijv. via e-mail)) voor zover dergelijke instructies consistent zijn met de voorwaarden van de Overeenkomst."*[53]

De DPA definieert persoonsgegevens als:

> *"…alle informatie die betrekking heeft op (i) een geïdentificeerde of identificeerbare natuurlijke persoon en, (ii) een geïdentificeerde of identificeerbare rechtspersoon (wanneer dergelijke informatie op vergelijkbare wijze als persoonsgegevens of persoonlijk identificeerbare informatie wordt beschermd onder toepasselijke wet- en regelgeving inzake gegevensbescherming), waarbij voor elk van (i) of (ii) geldt dat dergelijke gegevens Klantgegevens zijn."*[54]

Dit betekent dat de doelbeperking van artikel 2.2 alleen van toepassing is op persoonsgegevens die deel uitmaken van de Klantgegevens.

Volgens Bijlage 2 van de Data Processing Addendum is deze van toepassing op onder andere Gebruikers van de Diensten en op persoonsgegevens waaronder namen, titels en beroepsgegevens, alsmede bijzondere categorieën persoonsgegevens. De lijst van betrokkenen en persoonsgegevens waarop de DPA van toepassing is, is niet-uitputtend.

Salesforce verstrekt een lijst van hun subverwerkers in hun document 'Salesforce Infrastructure and Sub-processors'. In deze lijst zijn de locaties opgenomen waar Salesforce gegevens verwerkt en/of opslaat voor elke subverwerker. Een van de subverwerkers van Salesforce voor HR2day is AWS, omdat het platform waarop HR2day draait volledig wordt gehost op AWS-infrastructuur. Om op de hoogte te worden gesteld van nieuwe subverwerkers van Salesforce dient u zich aan te melden voor notificaties.[55]

[50] https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/no-index/reseller-dpa.pdf
[51] Artikel 11.4 van de Platform Solution Reseller Agreement tussen Salesforce en HR2day.
[52] E-mail van Salesforce, 17 juli 2025.
[53] Artikel 2.2 van de Salesforce DPA.
[54] Artikel 1 van de Salesforce DPA.
[55] Abonneren op notificaties van nieuwe subverwerkers, https://www.salesforce.com/form/other/trust-compliance/?d=pb, geraadpleegd op 14 oktober 2025.

### 7.2.2 SignRequest

HR2day heeft een dienstverleningsovereenkomst en een subverwerkersovereenkomst met SignRequest B.V., gevestigd in Amsterdam, Nederland. Gebruikers moeten echter ook de privacyverklaring en de algemene voorwaarden van SignRequest accepteren wanneer zij gebruik willen maken van de functionaliteit voor het ondertekenen van contracten die SignRequest biedt.

### 7.2.3 Workbee

HR2day heeft een dienstverleningsovereenkomst en een subverwerkersovereenkomst met Workbee B.V. Workbee is gevestigd in Hilversum, Nederland.

### 7.2.4 Infor

HR2day heeft een dienstverleningsovereenkomst en een subverwerkersovereenkomst met Infor (Barneveld) B.V.

### 7.2.5 Expo

Tijdens het technisch onderzoek ontdekte SURF dat HR2day Expo gebruikt voor het verzenden van notificaties aan gebruikers. HR2day heeft de Data Processing Addendum gedeeld die het heeft afgesloten met het in de VS gevestigde 650 Industries Inc. (Expo). Volgens een online bron is 650 Industries Inc. gevestigd in Palo Alto, Californië, maar SURF heeft dit niet kunnen verifiëren.[56]

[56] https://www.verif.com/en/company/650-Industries-Inc--68d9b5d212992303386247ce/, geraadpleegd op 23 januari 2026.

### 7.2.6 ValidSign

ValidSign B.V. is een subverwerker die HR2day gedurende het uitvoeren van deze DPIA in gebruik heeft genomen. SURF heeft het niet kunnen opnemen in de technische tests. HR2day heeft wel een geldige dienstverleningsovereenkomst en subverwerkersovereenkomst met ValidSign.

## 7.3 Ontvangers

Alle subverwerkers die zijn beschreven in 7.2 kunnen worden gekwalificeerd als ontvangers. Wanneer instellingen en HR2day wettelijk verplicht zijn persoonsgegevens te verstrekken aan overheidsinstanties, zijn deze ook ontvangers.

Daarnaast werden tijdens de testscenario's eindpunten aangetroffen waarmee gegevens werden uitgewisseld. Een eindpunt is elk apparaat, elke dienst of elke applicatie die is verbonden met een netwerk en die gegevens kan verzenden of ontvangen. In dit geval zijn dit eindpunten die betrokken zijn bij de communicatie tijdens het technisch onderzoek. SURF heeft het gebruik van de volgende eindpunten kunnen koppelen aan het gebruik van de SignRequest-diensten. Het is echter niet duidelijk welke gegevens worden uitgewisseld en of dit persoonsgegevens van gebruikers omvat.

- sentry.sr-staging-1.com
- www.dropbox.com
- 62vqqh6qv58h.statuspage.io
- js.stripe.com
- www.googletagmanager.com
- www.gravatar.com
- www.google-analytics.com
- SignRequest-pro.s3.amazonaws.com
- cdn.prod.website-files.com
- cdnjs.cloudflare.com
- d3e54v103j8qbb.cloudfront.net
- assets.website-files.com
- fonts.googleapis.com
- region1.google-analytics.com
- consent.cookiebot.com
- imgsct.cookiebot.com
- fonts.gstatic.com
- m.stripe.network
    - m.stripe.com

De subverwerkersovereenkomst met SignRequest bevat geen subverwerkers.

Een andere ontvanger van persoonsgegevens is Google. HR2day gebruikt de Google Maps-integratie om de reisafstand voor medewerkers te berekenen en deelt daartoe hun adressen met Google. Google mag deze gegevens uitsluitend voor dit doel verwerken, maar er is geen dienstverleningsovereenkomst of subverwerkersovereenkomst met Google. Het is daardoor onduidelijk of Google deze gegevens voor eigen doeleinden verwerkt.

De HR2day+ App kan worden geïnstalleerd via de Apple App Store en de Play Store. Als gevolg hiervan hebben Apple en Google een koppeling tussen het gebruik van de HR2day+ App en het Apple- en Google-account van de gebruiker. Dit is niet specifiek voor de HR2day+ App, maar geldt voor alle apps die via de Apple App Store worden aangeboden. HR2day heeft geen verwerkersovereenkomsten met Apple en Google getoond.

## 7.4 Overige verwerkingsverantwoordelijken

### 7.4.1 HR2day

HR2day stelt dat het bedrijf de van klanten verkregen persoonsgegevens uitsluitend verwerkt in haar hoedanigheid als verwerker en deze gegevens derhalve niet verwerkt voor door haar zelf bepaalde doeleinden en middelen.

De privacyverklaring van HR2day toont echter dat HR2day verwerkt:

- "Persoonlijke basisinformatie zoals naam, adres, telefoonnummer, e-mailadres en demografische informatie
- Informatie over de gebruiker en het webverkeer zoals inloggegevens, gebruikersnaam en IP-adres
- Inhoud die u heeft geüpload of verstrekt zoals foto's, reacties, artikelen en video's
- Statistieken die laten zien hoe gebruikers onze software gebruiken en de toestemming die wij aanbieden."[57]

Deze persoonsgegevens worden rechtstreeks verzameld van personen die werkzaam zijn bij hun klanten en bij gebruik van de website, wat gebruikers van de HR2day-applicatie kunnen zijn. Het is onduidelijk of deze gegevens worden verzameld voor de doeleinden die in de privacyverklaring worden vermeld, of dat HR2day verwerkingsactiviteiten uitvoert met persoonsgegevens die oorspronkelijk voor de doeleinden van de instellingen via de applicatie zijn verzameld.

De gegevens worden – onder meer – gebruikt voor de volgende doeleinden:

- "Verbeteren en (verder) ontwikkelen van de kwaliteit, functionaliteit en gebruikerservaring van onze producten, diensten en de HR2day-website
- Aanbieden van klantondersteuning voor onze producten en diensten
- Opsporen, verhelpen en voorkomen van bedreigingen voor en misbruik van de beveiliging, uitvoeren van onderhoud en verwijderen van bugs
- Beheren van marketingvoorkeuren en sturen van marketingcontent

- Aanmaken van belangstellingsprofielen voor het promoten van relevante producten en diensten (profilering)"[58]

Deze doeleinden zijn niet beschreven in de verwerkersovereenkomsten. Het feit dat deze persoonsgegevens en doeleinden worden vermeld in de privacyverklaring van HR2day is ook een aanwijzing dat de instellingen HR2day niet hebben geïnstrueerd om deze verwerkingsactiviteiten uit te voeren.

Gebruikerstevredenheid

HR2day verzamelt gebruikerstevredenheidsbeoordelingen via pop-ups in de applicatie ten behoeve van serviceverbetering. Gebruikers ontvangen de pop-ups eens per zes maanden. Als ze deze negeren, verschijnt de pop-up na twee maanden opnieuw en als ze reageren, verschijnt deze na zes maanden opnieuw. Ze kunnen de applicatie een beoordeling geven en een opmerking achterlaten. HR2day bepaalt welke gegevens worden verzameld en slaat deze op samen met het e-mailadres van de gebruiker voor een periode van drie jaar. Instellingen kunnen deze functionaliteit niet uitschakelen, hebben geen toegang tot deze gegevens en kunnen niet sturen wat HR2day verzamelt. Na drie jaar wordt het e-mailadres uit de beoordeling verwijderd. 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. HR2day dient daarom te worden gekwalificeerd als verwerkingsverantwoordelijke hiervoor.

[57] Privacyverklaring HR2day, geraadpleegd op 18 mei 2025.

[58] Privacyverklaring HR2day.

### 7.4.2 Salesforce

Salesforce is de eigenaar van het Lightning-platform, een integraal onderdeel van het HR2day-product, en heeft een eigen privacyverklaring. Deze verklaring is alleen van toepassing wanneer Salesforce persoonsgegevens verwerkt als verwerkingsverantwoordelijke, niet op persoonsgegevens die vrijwillig worden ingediend bij hun diensten als geautoriseerde gebruiker. Omdat de Salesforce DPA geen bepalingen bevat over het recht van Salesforce om de gegevens die zij als verwerker verwerkt voor eigen doeleinden te gebruiken, zou de privacyverklaring geen betrekking moeten hebben op persoonsgegevens die onder de DPA vallen.

Volgens de privacyverklaring kan Salesforce via logbestanden en andere technologieën informatie verzamelen over de apparaten van gebruikers en hun gebruik van de diensten van Salesforce, waarvan een deel kan kwalificeren als persoonsgegevens (waaronder Gebruiksgegevens) als verwerkingsverantwoordelijke wanneer gebruikers hun producten en diensten gebruiken en ermee interacteren.[59] Omdat het Lightning-platform een van de diensten van Salesforce is, is deze situatie van toepassing op HR2day. Wanneer Salesforce op deze wijze persoonlijke (logging)gegevens verzamelt, verwerkt het deze voor eigen doeleinden als verwerkingsverantwoordelijke. Deze doeleinden omvatten het ontwikkelen en inzetten van AI-systemen en het combineren van de persoonsgegevens met persoonsgegevens die uit andere bronnen zijn verkregen. In andere documentatie stelt

Salesforce dat het het gebruik van de dienst kan volgen en analyseren voor beveiligings- en serviceverbeteringsdoeleinden.[60] HR2day heeft een overzicht verstrekt van de logging die zij Salesforce hebben opgedragen uit te voeren met behulp van hun functionaliteit. Het is onduidelijk of deze logging en de bijgehouden gebruiksgegevens vallen onder de definitie van Klantgegevens en worden gedekt door de Salesforce DPA of niet. Op basis van de in de privacyverklaring vermelde doeleinden kan worden aangenomen dat Salesforce meer loggegevens verwerkt als verwerkingsverantwoordelijke dan de typen die in de HR2day-documentatie zijn vermeld. Het is onduidelijk wat deze verwerking inhoudt en welke persoonsgegevens deze kan bevatten. Volgens Salesforce verwerken zij de Gebruiksgegevens op een wijze die het niet mogelijk maakt individuen te identificeren (zie 4.3.10.1 Salesforce).

Salesforce gebruikt ook een aantal cookies om persoonsgegevens te verzamelen, die niet worden gedekt door de DPA en waarvoor geen openbare documentatie beschikbaar is. Het is onduidelijk of sommige doeleinden van deze cookies de reikwijdte van het leveren van de diensten van Salesforce overschrijden. Door het gebrek aan transparantie hebben instellingen – via HR2day – geen mogelijkheid om het gebruik van deze cookies goed te keuren en Salesforce instructies te geven over het gebruik van deze cookies.

[59] Volledige Salesforce Privacy Statement, https://www.salesforce.com/company/legal/privacy/#privacy-statement, geraadpleegd op 15 oktober 2025.

[60] Hyperforce Security, Privacy and Architecture, p. 13.

# 8 Belangen bij de gegevensverwerking

## 8.1 Onderwijs- en onderzoeksinstellingen

Deze instellingen hebben belang bij een HR- en salarisadministratiesysteem dat hen in staat stelt hun wettelijke verplichtingen als werkgever na te komen – inclusief verplichtingen op het gebied van gegevensbescherming – en de effectieve, efficiënte en veilige werking van hun bedrijfsprocessen te ondersteunen. Zij hebben ook een financieel belang bij het voorkomen van handhaving door juridische autoriteiten en een belang bij het beschermen van hun reputatie als betrouwbare instellingen.

## 8.2 HR2day

HR2day wordt gebruikt door ongeveer 15-20 hogescholen en ongeveer 5-10 mbo-instellingen. Het bedrijf heeft een commercieel belang bij het behouden en uitbreiden van dit marktaandeel door onder meer betrouwbare en hoogwaardige diensten te leveren. Daarnaast heeft het een belang bij naleving van wet- en regelgeving zoals de AVG en bij een reputatie als betrouwbare aanbieder van HR- en salarisverwerkingsdiensten.

## 8.3 Subverwerkers

Subverwerkers hebben een commercieel belang bij het behouden van HR2day als klant door het leveren van kwaliteitsdiensten en het stellen van het bedrijf in staat wet- en regelgeving na te leven. Zij hebben ook belang bij het naleven van wet- en regelgeving en het beschermen van hun reputatie.

Salesforce, als de subverwerker die de gehele HR2day-applicatie host, is een bijzonder belangrijke subverwerker voor HR2day. Salesforce heeft een commercieel belang bij het behouden van HR2day als klant. Vanwege zijn enorme omvang en mondiale bereik is de afhankelijkheid van Salesforce van HR2day als klant echter veel kleiner dan andersom.

### 8.3.1 Apple en Google

Zoals beschreven in paragraaf 1.4 HR2day+ App zijn Apple en Google betrokken als mogelijke subverwerkers voor de mobiele app. Apple en Google zijn betrokken als distributeurs van de mobiele app via hun app stores, waarbij gegevensverwerking plaatsvindt binnen hun eigen commerciële kaders en belangen. Zie voor meer informatie 16.17 Verlies van controle over verwerkte persoonsgegevens door het installeren van de mobiele app via een app store van een derde partij.

## 8.4 Betrokkenen

De docenten, niet-bezoldigde personeelsleden en andere betrokkenen van wie de persoonsgegevens worden verwerkt in HR2day, hebben belang bij een zorgvuldige en (AVG-)conforme omgang met hun gegevens. Zij hebben ook belang bij een goed functionerend HR-

systeem bij hun werkgever, waarmee zij toegang hebben tot de gegevens die zij nodig hebben voor hun werk en waarmee zij hun HR- en salarisrechtelijke aanspraken kunnen uitoefenen.

# 9 Verwerkingslocaties en gegevensdoorgiften

## 9.1 Salesforce

De HR2day-applicatie en de bijbehorende databases zijn opgeslagen op de Hyperforce-infrastructuur van Salesforce, die wordt gehost op AWS-infrastructuur.[61] HR2day heeft gekozen voor de datacenters van Salesforce in Parijs en Frankfurt voor het hosten van de klantgegevens die worden verwerkt bij het gebruik van HR2day. Niet-klantgegevens, zoals controllergegevens van Salesforce, kunnen echter het land van de gekozen datacenters verlaten.[62] De verwerkersovereenkomsten van de instellingen met HR2day bevatten beschrijvingen van mogelijke gegevensdoorgiften als gevolg van het gebruik door HR2day van de diensten van Salesforce en vermelden dat de verwerking van persoonsgegevens plaatsvindt in de landen waar de datacenters zich bevinden.

In de volgende paragrafen worden de mogelijke gegevensdoorgiften beschreven die plaatsvinden als gevolg van het gebruik van de diensten van Salesforce. Conform de EDPB is sprake van een doorgifte wanneer:

1) "Een verwerkingsverantwoordelijke of een verwerker ('exporteur') is onderworpen aan de AVG voor de betreffende verwerking.

2) De exporteur maakt door verstrekking of anderszins persoonsgegevens, die onderworpen zijn aan deze verwerking, beschikbaar aan een andere verwerkingsverantwoordelijke, gezamenlijke verwerkingsverantwoordelijke of verwerker ('importeur').

3) De importeur bevindt zich in een derde land, ongeacht of deze importeur al dan niet onderworpen is aan de AVG voor de betreffende verwerking overeenkomstig artikel 3, of is een internationale organisatie."[63]

HR2day is onderworpen aan de AVG voor de verwerking van persoonsgegevens in HR2day en kwalificeert als exporteur wanneer het deze persoonsgegevens verstrekt aan Salesforce. Omdat HR2day een overeenkomst heeft met Salesforce Inc., gevestigd in de VS, kwalificeert Salesforce als importeur in een derde land als HR2day persoonsgegevens verstrekt.

[61] https://help.salesforce.com/s/articleView?id=000396845&type=1, 20 mei 2025
[62] https://help.salesforce.com/s/articleView?id=000795008&type=1, 20 mei 2025
[63] Richtsnoeren 05/2021 over de wisselwerking tussen de toepassing van artikel 3 en de bepalingen over internationale doorgiften zoals bedoeld in hoofdstuk V van de AVG, EDPB, p. 7

### 9.1.1 Verzoeken van opsporingsautoriteiten

De klantgegevens, inclusief persoonsgegevens, alsmede de back-ups worden gehost in de datacenters van Salesforce binnen de EER. Deze gegevens zijn versleuteld at rest en in transit. De encryptiesleutels worden beheerd door Salesforce. Wanneer de persoonsgegevens zijn opgeslagen in datacenters in de EER, zonder dat Amerikaanse autoriteiten er op een redelijke manier toegang toe hebben, vormt het enkele risico van toegang door buitenlandse autoriteiten geen doorgifte.[64] Wanneer Salesforce een juridisch bindend verzoek tot toegang tot persoonsgegevens ontvangt van een overheidsinstantie, heeft het de stappen vermeld die

het zal ondernemen om de klant te informeren en het bevel te betwisten.[65] Salesforce garandeert ook dat het geen overheidsinstantie encryptiesleutels zal verstrekken en dat het geen achterdeurtjes inbouwt in zijn producten.[66] Salesforce heeft echter eerder inhoudelijke en niet-inhoudelijke gegevens verstrekt aan overheidsinstanties en heeft niet gegarandeerd dat het nooit persoonsgegevens van EU-klanten in de onderwijssector heeft verstrekt. Volgens het transparantierapport, dat alleen verzoeken omvat die betrekking hebben op klantgegevens, heeft Salesforce in 86% van de gevallen gegevens verstrekt in reactie op 136 verzoeken. De DPA bevat ook geen 'canary clause' die garandeert dat Salesforce hun klant (HR2day) informeert wanneer het niet meer in staat is te voldoen aan (een specifieke bepaling in) de DPA, zoals het betwisten van een verzoek van een opsporingsautoriteit, zonder de reden hiervoor te hoeven vermelden.

[64] https://www.edps.europa.eu/system/files/2023-07/2023-07-13-edps-cjeu-cisco-decision_en.pdf, 20 mei 2025

[65] Artikel 8.1 van de Salesforce DPA.

[66] Salesforce Transparancy Report, 14 maart 2025, https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/2024-transparency-report.pdf, geraadpleegd op 17 oktober 2025.

### 9.1.2 Klantondersteuning en technische operationele ondersteuning

Standaard wordt ondersteuning verleend door medewerkers binnen de EU en heeft Salesforce geen toegang tot de HR2day-omgeving van instellingen, tenzij de instelling hier toestemming voor geeft. Wanneer HR2day echter Salesforce toestemming geeft om in hoogprioritaire gevallen 24/7 ondersteuning te verlenen, kunnen instellingen toegang verlenen tot klantgegevens aan ondersteuningsmedewerkers van buiten de EU als de instelling hiervoor toestemming geeft, voor een bepaalde periode. Deze DPIA gaat ervan uit dat de mogelijkheid van gegevensdoorgiften voor ondersteuning is gedekt in de verwerkersovereenkomst tussen HR2day en instellingen, op basis van de steekproef van geïnspecteerde verwerkersovereenkomsten.

Wanneer HR2day persoonsgegevens verstrekt aan ondersteuningsmedewerkers van Salesforce of van een van hun subverwerkers door hen via ondersteuningsverzoeken toegang te verlenen tot deze gegevens, vormt dit een doorgifte. Salesforce kan ook medewerkers van hun subverwerkers toegang verlenen tot deze gegevens. Deze subverwerkers bevinden zich in:

- Verenigde Staten (adequaatheidsbesluit)
- Argentinië (adequaatheidsbesluit)
- Australië
- Oostenrijk
- Brazilië (adequaatheidsbesluit)
- Canada (adequaatheidsbesluit)
- Frankrijk
- Duitsland
- India

• Ierland
• Israël (adequaatheidsbesluit)
• Italië
• Japan (adequaatheidsbesluit)
• Nederland
• Singapore
• Zuid-Korea
• Spanje
• Zweden
• Zwitserland
• Thailand
• Verenigd Koninkrijk (adequaatheidsbesluit)[67]

[67] Salesforce Infrastructure and Sub-Processors, https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/misc/salesforce-infrastructure-and-subprocessors.pdf, p. 4, geraadpleegd op 15 oktober 2025.

### 9.1.3 Technische operationele ondersteuning

Om technische of serviceproblemen op te lossen, kan een team van Salesforce-databasebeheerders incidenteel op afstand toegang nodig hebben tot de databasetabellen waarop de persoonsgegevens van klanten worden gehost, volgens "strikte toegangs- en monitoringcontroles".[68] De subverwerkers die Salesforce hiervoor kan inschakelen, bevinden zich op dezelfde locaties als de lijst in 9.1.2.

Salesforce noemt de volgende doeleinden hiervoor:

- Beheer van servers, verbindingen en netwerken
- Verlenen van technische en netwerkdiensten
- Onderhoud van operaties
- Verhelpen van hardwareproblemen
- Kwaliteitsborgingstests

Deze doeleinden zijn ook gedekt in de verwerkersovereenkomst tussen HR2day en instellingen.

Conform de DPA tussen HR2day en de instellingen zijn de volgende maatregelen getroffen ter bescherming van persoonsgegevens.

- Gebruik van software die het kopiëren/plakken en afdrukken van gegevens blokkeert
- Goedkeuring van senior management
- Documentatie van toegangsverzoeken en logging van toegang
- Kwartaalmatige beoordeling van toegang
- Blokkering van toegang bij beëindiging van het dienstverband

- Meerdere authenticatieniveaus

Bovendien is de gegevensopslag in Salesforce zodanig ingericht dat de gegevens geen waarde hebben zonder de applicatielogica.

- Voor- en achternamen worden niet samen opgeslagen, en hetzelfde geldt voor identificatiecodes zoals burgerservicenummers. Iemand die toegang heeft tot de database weet derhalve niet welke gegevens hij/zij bekijkt.
- De gegevens en de applicatielogica worden afzonderlijk opgeslagen. Dit is een fundamenteel onderdeel van de algehele architectuur van het Salesforce-platform. Het gevolg is dat ongeoorloofde toegang tot de database geen toegang biedt tot bruikbare gegevens.

SURF heeft deze maatregelen niet kunnen verifiëren, maar zij maken deel uit van de contractuele afspraken tussen HR2day en instellingen in de steekproef van SURF.

[68] Salesforce Transfer Impact Assessment White Paper, https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/Agreements/SFDC-Online-Transfer-Risk-Assessment-Whitepaper-for-Customers-(Salesforce-Services)-February-2022.pdf, geraadpleegd op 28 januari 2026, p. 7.

### 9.1.4 Replicatie van gebruikersinformatie (User Information Replication)

Salesforce legt uit: "Wanneer Gebruikers inloggen in de Salesforce-omgeving van de Klant, worden inlogverzoeken verzonden naar het dichtstbijzijnde datacenter voor authenticatie. Het authenticatieproces stuurt de Gebruiker door naar het juiste datacenter voor de duur van de actieve sessie. Salesforce kan tijdelijk identificerende informatie over Gebruikers opslaan in haar gegevensopslaglocaties buiten Europa met als doel het inlogproces te faciliteren, zelfs als alle persoonsgegevens zijn opgeslagen binnen Europa."[69] Wanneer de MyDomain-functie is ingeschakeld, kan de mogelijkheid voor gebruikers om in te loggen via https://login.salesforce.com en https://welcome.salesforce.com worden uitgeschakeld, waardoor identificerende gegevens niet buiten Europa worden opgeslagen via het inlogproces, omdat gebruikers worden gedwongen hun eigen aangepaste URL te gebruiken (hr2day-xxxx.salesforce.com).

SURF heeft geen bewijs ontvangen dat deze instellingen waren uitgeschakeld in MyDomain.

[69] Salesforce Transfer Impact Assessment White Paper, https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/Agreements/SFDC-Online-Transfer-Risk-Assessment-Whitepaper-for-Customers-(Salesforce-Services)-February-2022.pdf, geraadpleegd op 28 januari 2026, p. 7, 8.

### 9.1.5 Content Delivery Networks (CDN)

Salesforce stelt:

> *"Content delivery networks ('CDN's') worden gebruikt voor het optimaliseren van de contentlevering voor bepaalde Salesforce-diensten zoals vermeld in de Salesforce Infrastructure & Sub-processor Documentatie. CDN's zijn veelgebruikte systemen van gedistribueerde diensten die de overdracht van content versnellen. Doorgaans wordt*

*een CDN gebruikt om beveiligd kopieën van content wereldwijd op te slaan in de cache, ter betere ondersteuning van eindgebruikers van de betreffende Salesforce-diensten. Salesforce maakt het gebruik van bepaalde CDN's mogelijk in combinatie met de Salesforce-diensten."*[70]

De Salesforce Infrastructure & Sub-processor Documentatie vermeldt dat Salesforce wereldwijde CDN's gebruikt, waarbij gebruik wordt gemaakt van de subverwerkers Akamai Technologies, Inc., Amazon Web Services, Inc. en Cloudflare. Deze kunnen gegevens verwerken in elk land, ongeacht de locatie van de klant, en zij sturen openbaar cacheable content, statische resources (zoals HTML-pagina's, JavaScript- en CSS-bestanden, afbeeldingen en lettertypebestanden) en andere cacheable webpaginacontent.[71] Het is onduidelijk of de gecachede content persoonsgegevens bevat die door instellingen zijn ingediend. Volgens Salesforce verloopt alle communicatie tussen hun CDN-partner en Salesforce via HTTPS.[72] HR2day gebruikt de standaard cache-instelling, wat betekent dat de gegevens minimaal vijf minuten en maximaal tien minuten worden gecached.

[70] Salesforce Transfer Impact Assessment White Paper, https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/Agreements/SFDC-Online-Transfer-Risk-Assessment-Whitepaper-for-Customers-(Salesforce-Services)-February-2022.pdf, geraadpleegd op 28 januari 2026, p. 8.

[71] Salesforce Infrastructure and Sub-processors, https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/misc/salesforce-infrastructure-and-subprocessors.pdf, geraadpleegd op 28 januari 2026, p. 3, 64, 65.

[72] Considerations for the Salesforce CDN, https://help.salesforce.com/s/articleView?id=platform.community_builder_cdn_considerations.htm&type=5, geraadpleegd op 28 januari 2026.

## 9.2 Mogelijke aanvullende doorgiften

Tijdens het technisch onderzoek werden eindpunten van derden aangetroffen die zich bevinden in landen buiten de EER. Sommige hiervan kunnen worden toegeschreven aan de hierboven beschreven doorgiften en sommige zijn het gevolg van verwerking door Google, Expo en SignRequest. Het is onduidelijk of persoonsgegevens worden doorgegeven aan de organisaties die verantwoordelijk zijn voor deze eindpunten of dat deze organisaties zelf doorgiften uitvoeren. In de verwerkersovereenkomsten is geen verwerking buiten de EER gedocumenteerd, anders dan de doorgiften aan Salesforce.

## 9.3 Doorgiftemechanismen

Momenteel is een adequaatheidsbesluit van de Europese Commissie – het Data Privacy Framework – van toepassing op doorgiften tussen de EER en de VS. Salesforce is gecertificeerd onder het DPF, zodat de doorgiften van persoonsgegevens aan Salesforce als subverwerker een adequaat beschermingsniveau kennen. Omdat echter de voorzitter en twee andere leden van de US Privacy and Civil Liberties Oversight Board (PCLOB), een kernpijler van het DPF, zijn ontslagen, staat het adequaatheidsbesluit onder druk.

Salesforce beschikt ook over binding corporate rules voor processors (BCR-P).[73] Binding corporate rules zijn in wezen een geheel van gegevensbeschermingsbeleid waaraan alle

bedrijven binnen een groep zich houden en dat is goedgekeurd door de relevante toezichthouder en door de EDPB. Deze BCR-P zijn van toepassing op internationale doorgiften van persoonsgegevens naar en tussen leden van de Salesforce Group, waaronder alle subverwerkers van Salesforce.

Ten slotte maken de standaardcontractbepalingen (SCC's) van de Europese Commissie deel uit van het contractuele kader tussen instellingen en HR2day, zodat zij van toepassing zijn op alle doorgiften die HR2day uitvoert. Op dit moment hoeft HR2day hier niet op te steunen om een adequaat beschermingsniveau te garanderen. Als het DPF wordt ingetrokken, dient HR2day een DTIA uit te voeren voor haar doorgiften.

[73] https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/misc/Salesforce-Processor-BCR.pdf, 20 mei 2025.

# 10 Bewaartermijnen en verwijdering

## 10.1 HR2day als verwerker

Instellingen zijn verantwoordelijk voor het bepalen en afdwingen van de bewaartermijnen voor de persoonsgegevens waarvoor zij verwerkingsverantwoordelijke zijn.

In HR2day kunnen gebruikers met het vereiste toegangsniveau gegevens(sets) verwijderen. Zij kunnen algemene en specifieke vervaldatums instellen voor documenten. De huidige manier van het verwijderen van gegevens verloopt via 'signaallijsten'. Deze lijsten worden periodiek gegenereerd, dat wil zeggen elk kwartaal, en bevatten alle gegevens (gebruikers, datasets, delen van datasets) die zouden moeten worden verwijderd. Via deze lijsten kunnen deze datasets handmatig worden verwijderd door een gebruiker met het profiel 'extra rechten'. Dit profiel staat alleen toe deze documenten te verwijderen, niet om ze in te zien.

HR2day heeft contact opgenomen met haar klanten over hoe bewaartermijnen beter kunnen worden ondersteund, geautomatiseerd en afgedwongen. Vooralsnog heeft de uitkomst van deze gesprekken geleid tot de conclusie dat de huidige werkwijze nog steeds voldoet aan de behoeften van de instellingen/klanten. De voornaamste redenering hierachter is:

- Het is een goed leesbaar en daarmee toegankelijk rapport.
- Instellingen/klanten zijn terughoudend ten aanzien van automatisch verwijderen. Zij geven de voorkeur aan een mens in de loop.

HR2day is in staat automatisering in dit proces te ontwikkelen, maar heeft van haar klanten geen instructies ontvangen om dit te doen.

*Zie voor meer informatie 16.14 Verlies van controle over bewaartermijnen door gebrek aan automatisering.*

### 10.1.1 Salesforce-klantgegevens

Artikel 9 van de Salesforce DPA verwijst naar de volgende informatie:

> *"Na beëindiging van alle abonnementen die verband houden met een van de Covered Services ('Subscription Termination') kunnen de Klantgegevens die zijn ingediend bij de Covered Services gedurende maximaal 120 dagen in een inactieve status blijven. Na deze periode worden de Klantgegevens binnen 90 dagen overschreven of verwijderd uit de productieomgeving. De Klantgegevens worden binnen 300 dagen na Subscription Termination verwijderd uit de back-ups. Dit proces is onderworpen aan toepasselijke wettelijke vereisten.*
>
> *Onverminderd de mogelijkheid voor klanten om teruggave te verzoeken van hun Klantgegevens die zijn ingediend bij de betreffende Covered Services, behoudt Salesforce zich het recht voor om het aantal dagen te verminderen dat dergelijke gegevens worden bewaard na beëindiging van de Covered Service. Salesforce zal deze Beveiligings-, Privacy- en Architectuurdocumentatie bijwerken in geval van een dergelijke wijziging."*[74]

[74] Hyperforce Security, Privacy and Architecture, https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/misc/hyperforce-security-privacy-and-architecture.pdf, p. 12, geraadpleegd op 17 oktober 2025.

### 10.1.2 Logging

Zie voor bewaartermijnen voor logging paragraaf 4.3.10 Logging.

### 10.1.3 Back-up

Zie voor bewaartermijnen voor back-ups paragraaf 5.8.

## 10.2 HR2day als verwerkingsverantwoordelijke

In haar privacyverklaring stelt HR2day dat het persoonsgegevens niet langer bewaart dan noodzakelijk voor haar doeleinden.

## 10.3 Salesforce

Zoals toegelicht in 4.3.10.1 verzamelt Salesforce gegevens[75], mogelijk persoonsgegevens, voor eigen doeleinden als een van de architectuurprincipes.

SURF heeft geen verdere documentatie ontvangen over deze logging-praktijken van Salesforce en kan daarom niet beoordelen of de bewaartermijnen gerechtvaardigd zijn.

[75] The Salesforce Platform - Transformed for Tomorrow, https://architect.salesforce.com/docs/architect/fundamentals/guide/platform-transformation.html, geraadpleegd op 2 april 2026.

# Deel B. Beoordeling van de rechtmatigheid van de gegevensverwerking

Het tweede deel van de DPIA beoordeelt de rechtmatigheid van de gegevensverwerking. Dit deel bevat een bespreking van de rechtsgrondslagen, een beoordeling van de noodzakelijkheid en evenredigheid van de verwerking, en van de verenigbaarheid van de verwerking in relatie tot de doeleinden.

# 11 Rechtsgrondslagen

Om toelaatbaar te zijn onder de AVG moet een verwerkingsverantwoordelijke de verwerking van persoonsgegevens baseren op een van de grondslagen zoals vermeld in artikel 6 lid 1 AVG. Deze grondslagen zijn:

a. de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;
b. de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
c. de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
d. de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;
e. de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;
f. de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is.

De beoordeling van beschikbare rechtsgrondslagen is nauw verbonden met het beginsel van doelbinding. De EDPB merkt op dat:

> *"De identificatie van de passende rechtsgrondslag is verbonden met de beginselen van eerlijkheid en doelbinding. [...] Wanneer verwerkingsverantwoordelijken de juiste rechtsgrondslag proberen te identificeren in lijn met het eerlijkheidsbeginsel, zal dit moeilijk te bereiken zijn als zij niet eerst duidelijk de doeleinden van de verwerking hebben vastgesteld, of als de verwerking van persoonsgegevens verder gaat dan wat noodzakelijk is voor de gespecificeerde doeleinden."*[76]

Om te bepalen of een rechtsgrondslag beschikbaar is voor een specifieke verwerkingsactiviteit, is het derhalve noodzakelijk vast te stellen voor welke doeleinden de gegevens zijn of worden verzameld en (verder) verwerkt. Er moet voor elk van deze doeleinden een rechtsgrondslag zijn. De toepasselijke rechtsgrondslag is bovendien afhankelijk van de rol van de instellingen en HR2day als verwerkingsverantwoordelijke of verwerker.

[76] EDPB, Richtsnoeren 2/2019 over de verwerking van persoonsgegevens op grond van artikel 6(1)(b) AVG in de context van het aanbieden van onlinediensten aan betrokkenen – versie vastgesteld na openbare raadpleging, 16 oktober 2019, URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en.

## 11.1 Rechtsgrondslagen instellingen

Instellingen zijn verwerkingsverantwoordelijke voor alle klantgegevens die worden verwerkt in de HR2day-processen zoals beschreven in hoofdstuk 4, met uitzondering van 4.3.10.1 Salesforce. Hieronder worden enkele mogelijke rechtsgrondslagen voor de instellingen besproken, alsook enkele bijbehorende aandachtspunten bij het toepassen van de rechtsgrondslag. Elke instelling dient haar eigen rechtsgrondslagen te bepalen op basis van haar specifieke verwerking.

**Rechtsgrondslag e: taak van algemeen belang**

Instellingen hebben een wettelijke verplichting om een publieke taak uit te voeren, namelijk het organiseren van onderwijs. Om zich op deze grondslag te beroepen, moeten instellingen een noodzakelijkheidstoets uitvoeren om aan te tonen dat de verwerking noodzakelijk is voor de goede uitvoering van hun publieke taak. Voor de verwerking van gegevens die niet noodzakelijk zijn voor hun publieke taak, kunnen instellingen mogelijk een beroep doen op een van de volgende grondslagen.

**Rechtsgrondslag a: toestemming**

Instellingen voeren de verwerking van HR- en salarisgegevens doorgaans uit in de rol van werkgever. Als zodanig bestaat er een machtsongelijkheid tussen hen en de betrokkenen, wat betekent dat betrokkenen niet vrij kunnen instemmen met de gegevensverwerking. Instellingen dienen zich voor de verwerking in HR2day dan ook in het algemeen te onthouden van het gebruik van deze rechtsgrondslag.

**Rechtsgrondslag b: uitvoering van een overeenkomst**

De verwerking in HR2day zal waarschijnlijk noodzakelijk zijn voor de uitvoering van de arbeidsovereenkomst en overeenkomsten van opdracht met de medewerkers en niet-bezoldigde personeelsleden. Ook hier moeten instellingen een noodzakelijkheidstoets uitvoeren om aan te tonen dat het doel van de overeenkomst niet kan worden bereikt zonder de relevante verwerking van persoonsgegevens.

**Rechtsgrondslag f: gerechtvaardigd belang**

Verwerking die niet noodzakelijk is voor de uitvoering van een overeenkomst, kan noodzakelijk zijn voor de behartiging van de gerechtvaardigde belangen van de instelling. Om gebruik te maken van deze grondslag moeten instellingen beoordelen of zij (1) een gerechtvaardigd belang hebben, (2) de verwerking noodzakelijk is om dit belang te behartigen en (3) of de belangen van de instelling zwaarder wegen dan die van de betrokkenen.

## 11.2 Rechtsgrondslagen HR2day

HR2day beschrijft de verwerking van persoonsgegevens die het voor eigen doeleinden uitvoert in haar privacyverklaring. Het is onduidelijk of HR2day gebruikmaakt van gegevens die oorspronkelijk voor de doeleinden van de instellingen zijn verzameld, of dat HR2day deze gegevens verzamelt als onafhankelijke verwerkingsverantwoordelijke, om de redenen zoals

beschreven in 7.4.1 HR2day. In reactie op deze DPIA heeft HR2day aangegeven dat haar privacyverklaring niet van toepassing is op de HR2day-applicatie, maar op de verwerkingsactiviteiten die zij als onafhankelijke verwerkingsverantwoordelijke uitvoert. De privacyverklaring zelf maakt dit echter niet duidelijk aan. Wanneer HR2day een onafhankelijke verwerkingsverantwoordelijke is, is zij afhankelijk van haar eigen rechtsgrondslagen, zoals (ten minste gedeeltelijk) beschreven in de privacyverklaring.

Voor elke verdere verwerking die HR2day uitvoert met gegevens van instellingen voor andere doeleinden dan de overeengekomen doeleinden (hoofdzakelijk personeelsadministratie, zie 2 Doeleinden), bepaalt HR2day de middelen en doeleinden en kwalificeert zij als verwerkingsverantwoordelijke.[77] Instellingen dienen te beoordelen of de verwerking voor deze doeleinden verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.[78] Als dat het geval is, moeten de instellingen ook instemmen met de verdere verwerking in de verwerkersovereenkomsten die zij met HR2day sluiten. Bij deze beoordeling dienen de volgende criteria in aanmerking te worden genomen:

- a. een mogelijke link tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de voorgenomen verdere verwerking;
- b. de context waarin de persoonsgegevens zijn verzameld, met name wat betreft de verhouding tussen betrokkenen en de verwerkingsverantwoordelijke;
- c. de aard van de persoonsgegevens, met name of bijzondere categorieën persoonsgegevens worden verwerkt op grond van artikel 9, of persoonsgegevens die verband houden met strafrechtelijke veroordelingen en strafbare feiten worden verwerkt op grond van artikel 10;
- d. de mogelijke gevolgen van de voorgenomen verdere verwerking voor betrokkenen;
- e. het bestaan van passende waarborgen, zoals encryptie of pseudonimisering.

[77] Artikel 28(10) AVG.

[78] Artikel 6(4) AVG.

### 11.2.1 Gebruikerstevredenheid

Er bestaat geen directe link tussen het doel van personeelsadministratie en serviceverbetering via het verzamelen van gebruikerstevredenheidsbeoordelingen, hoewel serviceverbetering een betere personeelsadministratie in HR2day ten goede kan komen. (a) HR2day heeft geen directe contractuele relatie met HR2day-gebruikers, waardoor zij geen reden hebben te verwachten dat HR2day hun gegevens verwerkt voor eigen serviceverbetering, anders dan wat noodzakelijk is voor de dienstverlening aan de instelling waarbij de gebruiker hoort. (b) De verzamelde persoonsgegevens hebben een lage kans om bijzondere of gevoelige gegevens te bevatten. Dit kan echter niet worden uitgesloten vanwege het open tekstveld dat beschikbaar is om opmerkingen achter te laten. (c) De gevolgen voor betrokkenen kunnen verlies van controle en verlies van vertrouwelijkheid zijn. (d) SURF heeft niet kunnen verifiëren of de waarborgen van HR2day in dit proces aanwezig en effectief zijn. (e) Derhalve leidt de verwerking van gebruikerstevredenheidsgegevens door HR2day voor serviceverbetering tot een onverenigbare verdere verwerking van persoonsgegevens voor eigen

serviceverbeteringsdoeleinden van HR2day. Instellingen hebben geen mogelijkheid om deze functionaliteit uit te schakelen.

## 11.3 Rechtsgrondslagen Salesforce

Salesforce is heel duidelijk over zijn rol als verwerker voor de klantgegevens die onder de DPA vallen. Salesforce heeft echter ook een uitgebreide privacyverklaring over de verwerking van – onder meer – de gebruiksgegevens en loggegevens van gebruikers, wat ook wordt vermeld in hun document Hyperforce Security, Privacy and Architecture. Zoals beschreven in 4.3.10.1 Salesforce heeft het documentenonderzoek en het technisch onderzoek niet aangetoond om welke gegevens het precies gaat en of deze gegevens oorspronkelijk voor de doeleinden van de instellingen zijn verzameld. Omdat Salesforce deze gegevens echter alleen kan verwerken doordat instellingen (indirect) zijn diensten gebruiken voor eigen doeleinden, is het waarschijnlijk dat er ten minste enige verdere verwerking plaatsvindt. Zoals beschreven in 7.4.2 Salesforce omvatten de eigen doeleinden van Salesforce serviceverbetering, beveiliging en het ontwikkelen en inzetten van AI-systemen.[79] Als Salesforce persoonsgegevens van HR2day-gebruikers voor deze doeleinden verwerkt, dienen instellingen de beoordeling van verdere verwerking uit te voeren zoals beschreven in 11.2.

De privacyverklaring van Salesforce toont dat zij persoonsgegevens verwerken van eindgebruikers van hun diensten. Op dit moment kan SURF juridisch noch technisch uitsluiten dat deze (verdere) verwerking plaatsvindt voor HR2day-eindgebruikers. Instellingen zijn niet in staat een beoordeling van verdere verwerking uit te voeren zonder te weten of en welke persoonsgegevens Salesforce verwerkt voor eigen doeleinden, wat betekent dat er geen aantoonbare rechtsgrondslag kan zijn voor eventuele verdere verwerking door Salesforce.

[79] De volledige lijst van doeleinden is beschikbaar in de privacyverklaring (https://www.salesforce.com/company/legal/privacy/#privacy-statement, geraadpleegd op 29 januari 2026).

# 12 Bijzondere categorieën persoonsgegevens en gevoelige gegevens

## 12.1 Bijzondere categorieën persoonsgegevens

HR2day bevat meerdere typen bijzondere categorieën persoonsgegevens, omdat het een instrument voor HR- en salarisadministratie is.

De grootste groep betreft gezondheidsgegevens. HR2day kan worden gebruikt om verzuim wegens ziekte te registreren en informatie over het verzuim toe te voegen. Instellingen kunnen hun eigen classificaties voor verzuim definiëren. Deze classificaties mogen niet meer informatie bevatten over de gezondheid van een betrokkene dan noodzakelijk is voor de administratie van de werkgever. Werkgevers kunnen voor dit doel gebruikmaken van de bestaande richtlijnen.[80] Het is ook mogelijk om in een vrij tekstveld opmerkingen toe te voegen over het verzuim van een medewerker. Daarnaast zijn er veel classificaties die werkgevers aan medewerkers kunnen toewijzen met behulp van de ingebouwde informatie van HR2day over wettelijke regelingen, fiscale regelingen en cao's. Deze classificaties kunnen ook informatie bevatten over de gezondheid van medewerkers, bijvoorbeeld wanneer zij aangeven dat een medewerker recht heeft op (belasting)voordelen vanwege een arbeidsongeschiktheid of wanneer zij aangeven dat de werkgever het ziekengeld inhoudt.

De salarisgegevens van een medewerker kunnen ook politieke gegevens zijn, wanneer zij aangeven dat de medewerker politiek verlof heeft gekregen, en gegevens over vakbondslidmaatschap, wanneer zij aangeven dat de werkgever helpt bij het betalen van vakbondsbijdragen.

De nationaliteit in combinatie met de geboorteplaats en het geboorteland toont de raciale of etnische afkomst van een betrokkene en mag alleen op deze wijze worden verwerkt als dit noodzakelijk is voor de identificatie van een medewerker of voor het toepassen van positieve discriminatie.[81]

HR2day heeft meer open tekstvelden die mogelijk worden ingevuld met bijzondere categorieën persoonsgegevens. Standaard biedt HR2day maximaal tien open tekstvelden met een specifiek doel. Deze velden bevatten een informatiepictogram dat instellingen kunnen gebruiken om uit te leggen welk type gegevens het veld dient te bevatten. Bovendien kunnen open tekstvelden worden toegevoegd aan elk type workflow. Zo zou een manager bijvoorbeeld informatie over de gezondheid van een medewerker kunnen vastleggen in de notities van de functioneringsgesprekken.

Omdat er bijzondere categorieën persoonsgegevens worden verwerkt in HR2day, dienen instellingen een beroep te kunnen doen op een uitzondering op het verwerkingsverbod van artikel 9 om deze gegevens te kunnen verwerken. Een waarschijnlijke uitzondering voor ten minste een deel van de gezondheidsgegevens is artikel 9 lid 2 sub b AVG, wanneer "de verwerking noodzakelijk is met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied

van het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht". Dit is geïmplementeerd in artikel 30 lid 1 sub b van de Nederlandse uitvoeringswet van de AVG, dat werkgevers toestaat gezondheidsgegevens te verwerken als de verwerking noodzakelijk is voor:

a. een goede uitvoering van wettelijke voorschriften, pensioenregelingen of cao's waarbij aanspraken afhankelijk zijn gesteld van de gezondheidstoestand van de betrokkene; of
b. de reïntegratie van of begeleiding van werknemers of uitkeringsgerechtigden in verband met ziekte of arbeidsongeschiktheid.

De AP heeft richtlijnen gepubliceerd over wat wel en niet noodzakelijk is in 'De zieke werknemer'[82], waarvan de geldigheid is herbevestigd in haar boete aan CP&A.[83]

[80] Beleidsregels verwerking persoonsgegevens gezondheid zieke werknemers, https://wetten.overheid.nl/BWBR0037896/2016-04-29, geraadpleegd op 29 januari 2026.
[81] Autoriteit Persoonsgegevens, Personeelsdossier, https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/personeelsgegevens/personeelsdossier, geraadpleegd op 29 januari 2025.
[82] Autoriteit Persoonsgegevens, De zieke werknemers, https://www.autoriteitpersoonsgegevens.nl/uploads/imported/beleidsregels_de_zieke_werknemer.pdf, geraadpleegd op 15 oktober 2025.
[83] Autoriteit Persoonsgegevens, Boete CP&A verzuimregistratie, https://autoriteitpersoonsgegevens.nl/uploads/imported/boete_cpa_verzuimregistratie.pdf, geraadpleegd op 15 oktober 2025.

## 12.2 Gevoelige gegevens

De voornaamste categorie gevoelige gegevens zijn de financiële gegevens in de salarisadministratie. Deze gegevens tonen informatie over de financiële situatie van betrokkenen.

HR2day bevat gegevens over (wijzigingen in) het salaris van betrokkenen, aanvullende (reis)vergoedingen, pensioen, of er loonbeslag is gelegd en alle componenten – wettelijk en contractueel – die elk periode het salaris vormen. Er zijn ook veel vrije tekstvelden die per ongeluk ingevuld kunnen worden met gevoelige gegevens.

De AVG bevat geen aanvullende regels voor dit type gegevens, maar verwerkingsverantwoordelijken dienen bij het bepalen van de passende technische en organisatorische maatregelen die noodzakelijk zijn om te voldoen aan de AVG rekening te houden met het verhoogde risico van de verwerking van gevoelige gegevens.[84]

[84] Artikel 24 AVG.

## 12.3 Nationale identificatienummers

Werkgevers kunnen nationale identificatienummers (BSN's) van medewerkers en niet-bezoldigde personeelsleden verwerken in HR2day.

Nummers die worden gebruikt ter identificatie van een persoon en die bij wet zijn voorgeschreven, mogen uitsluitend worden verwerkt voor bij wet gespecificeerde doeleinden.

Het gebruik van deze nummers dient met de grootste zorgvuldigheid te worden uitgevoerd en de noodzaak van het gebruik van deze nummers dient goed te worden onderbouwd.[85] Bovendien vereist het Nederlandse recht dat het BSN uitsluitend mag worden gebruikt door overheidsorganen of door andere organisaties voor zover dit bij wet is voorgeschreven.[86] Werkgevers en opdrachtgevers mogen het BSN uitsluitend verwerken voor belastingdoeleinden onder strikte voorwaarden.[87]

[85] Artikel 87 AVG en artikel 46 lid 1 van de Nederlandse uitvoeringswet AVG.

[86] Artikel 1 sub d van de Wet algemene bepalingen burgerservicenummer (Wabb).

[87] Autoriteit Persoonsgegevens, BSN op werk, https://www.autoriteitpersoonsgegevens.nl/themas/identificatie/burgerservicenummer-bsn/bsn-op-het-werk, geraadpleegd op 16 oktober 2025.

# 13 Doelbinding

Het beginsel van doelbinding houdt in dat gegevens uitsluitend mogen worden "verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en niet verder worden verwerkt op een wijze die onverenigbaar is met die doeleinden; verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89 lid 1 niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd".[88] In wezen betekent dit dat de verwerkingsverantwoordelijke een gespecificeerd doel moet hebben waarvoor hij persoonsgegevens verzamelt, en deze gegevens uitsluitend mag verwerken voor doeleinden die verenigbaar zijn met dat oorspronkelijke doel. Verwerkingsverantwoordelijken moeten op grond van artikel 5 lid 2 AVG kunnen aantonen dat zij dit beginsel naleven (verantwoordingsplicht).

Het is aan de instellingen als verwerkingsverantwoordelijken om te bepalen voor welke doeleinden zij de gegevens in HR2day verwerken. Hoofdstuk 2 geeft een overzicht van waarschijnlijke doeleinden voor de verwerking in HR2day. Als verwerkers mogen HR2day en Salesforce persoonsgegevens uitsluitend verwerken voor de doeleinden die instellingen in de verwerkersovereenkomsten bepalen. Als HR2day en Salesforce persoonsgegevens verzamelen en verwerken voor eigen doeleinden als onafhankelijke verwerkingsverantwoordelijken, dienen zij aan te geven welke gegevens dit zijn en wat de doeleinden zijn. Als zij verdere verwerking uitvoeren, dienen zij instellingen te voorzien van de noodzakelijke informatie zodat deze kunnen aantonen dat de verwerking verenigbaar is met de oorspronkelijke doeleinden waarvoor de gegevens door de instellingen zijn verzameld. In 2 Doeleinden en 7.4 Overige verwerkingsverantwoordelijken zijn de andere doeleinden beschreven waarvoor HR2day en Salesforce mogelijk persoonsgegevens van betrokkenen verwerken. Deze DPIA heeft niet kunnen aantonen dat – in tegenstelling tot wat de privacyverklaring van Salesforce toont – Salesforce geen persoonlijke (gebruiks)gegevens van eindgebruikers verwerkt voor eigen doeleinden. De privacyverklaring van HR2day biedt ook geen volledige duidelijkheid over de vraag of HR2day persoonsgegevens verder verwerkt voor eigen doeleinden en zo ja, welke, met uitzondering van de verwerking door HR2day van gebruikerstevredenheidsgegevens voor serviceverbetering. Het gebrek aan transparantie van zowel HR2day als Salesforce over de mogelijke doeleinden waarvoor zij persoonsgegevens uit de applicatie verwerken, betekent dat instellingen niet aan hun verantwoordingsverplichtingen kunnen voldoen.

[88] Artikel 5 lid 1 sub b AVG.

# 14 Noodzakelijkheid en evenredigheid

Elke verwerkingsactiviteit moet voldoen aan de eisen van noodzakelijkheid en evenredigheid uit de AVG.

Om aan te tonen dat een verwerkingsactiviteit noodzakelijk is, dient een verwerkingsverantwoordelijke aan te tonen dat het een effectieve manier is om de beoogde doeleinden te bereiken en dat er geen minder ingrijpende manier bestaat om het beoogde doel te bereiken (subsidiariteit).

Om aan te tonen dat een verwerkingsactiviteit evenredig is, dient een verwerkingsverantwoordelijke aan te tonen dat de inbreuk op de privacy en de bescherming van de persoonsgegevens van betrokkenen evenredig is aan de doeleinden van de verwerking. Evenredigheid vereist een afweging tussen de belangen van de betrokkene en de verwerkingsverantwoordelijke.

Dit hoofdstuk onderzoekt of HR2day instellingen in staat stelt aan de eisen van noodzakelijkheid en evenredigheid te voldoen. Instellingen kunnen dit gebruiken om een volledige beoordeling uit te voeren op basis van de details van hun HRM- en salarisprocessen.

## 14.1 Effectiviteit en subsidiariteit

Om de noodzakelijkheid van de verwerkingsactiviteiten in HR2day te beoordelen, zal de DPIA onderzoeken of HR2day een effectief instrument is om de doeleinden zoals beschreven in hoofdstuk 2 te bereiken. Er zal ook een beoordeling plaatsvinden of er minder ingrijpende alternatieven (zoals andere instrumenten) beschikbaar zijn om dezelfde doeleinden te bereiken.

### 14.1.1 Effectiviteit

Het voornaamste doel van de instellingen is het snel en efficiënt kunnen uitvoeren van HRM-bedrijfsprocessen "in het belang van een verantwoord personeelsbeleid voor zowel individuen als de organisatie als geheel". Het hebben van een instrument dat human resources en salarisadministratie combineert en helpt processen te automatiseren en te stroomlijnen, is een effectieve manier om dit te bereiken.

### 14.1.2 Subsidiariteit

Om het doel van het uitvoeren van HRM-bedrijfsprocessen te bereiken, zullen de meeste instellingen tot de conclusie komen dat een HRM-applicatie zoals HR2day noodzakelijk is. De keuze voor welke applicatie te gebruiken heeft een grote impact op de ingrijpendheid van de verwerking van persoonsgegevens, omdat hiermee wordt bepaald met welke leverancier instellingen hun gegevens delen. Het feit dat Salesforce de volledige architectuur en hosting van HR2day verzorgt, betekent dat alle persoonsgegevens – klantgegevens, gebruiksgegevens, loggegevens, etc. – worden gedeeld met deze grote, in de VS gevestigde leverancier die gebruikmaakt van veel subverwerkers. De mogelijke verdere verwerking door Salesforce voegt toe aan de ingrijpendheid van de verwerking via HR2day. De mogelijkheid van verzoeken van

buitenlandse opsporingsautoriteiten, doordat Salesforce en zijn hostingpartijen in de VS zijn gevestigd, draagt ook bij aan de ingrijpendheid. Er kunnen andere leveranciers van HRM-applicaties zijn die geen dergelijke verdere verwerking uitvoeren en hun gegevens niet hosten bij in de VS gevestigde partijen, waardoor zij in deze opzichten minder ingrijpend zijn dan HR2day. Dit is iets waarmee instellingen rekening dienen te houden bij hun subsidiariteitsbeoordelingen.

Een ander punt is dat de HR2day+ mobiele app beschikbaar is via de Apple App Store en de Google Play Store. Wanneer een medewerker de app downloadt, wordt automatisch een koppeling gecreëerd tussen het gebruik van de app en het persoonlijke Apple- of Google-account van de medewerker. Dit betekent dat het hebben van een Apple-account of een Google-account noodzakelijk is om de app te gebruiken, waarmee deze platforms inzicht krijgen in het feit dat de app is geïnstalleerd en deze informatie kunnen combineren met de andere gegevens die zij waarschijnlijk al over de gebruiker hebben verzameld. Deze vorm van gegevensverwerking is niet strikt noodzakelijk voor het aanbieden van de app, omdat er minder privacyingrijpende alternatieven bestaan. Zo zou HR2day er bijvoorbeeld voor kunnen kiezen de app aan te bieden als zogenaamd 'sideload' buiten de reguliere app stores, waardoor de betrokkenheid van Google en Apple wordt geminimaliseerd, of het openen van HR2day in een browser mogelijk te maken.

De mobiele HR2day+ App verstuurt ook pushmeldingen. De pushmeldingen leiden zowel tot de overdracht van metadata als van inhoud naar Google en Apple. De metadata betreft gegevens zoals apparaat-ID's, IP-adressen en mogelijk het Google- of Apple-account van de medewerker. De inhoud betreft de berichten als die inhoud onversleuteld wordt verzonden, zoals noodzakelijkerwijs het geval is bij het "notification messages"-gedeelte van de pushmeldingen. De inhoud van deze berichten is zichtbaar voor en wordt verwerkt door Google en Apple. Instellingen bepalen zelf de inhoud van de berichten en kunnen privacyvriendelijke keuzes maken, bijvoorbeeld door geen persoonsgegevens op te nemen. Ongeacht de inhoud van de berichten betekent het gebruik van notification messages dat de inhoud van de berichten systematisch wordt verwerkt door Google. Dit kan worden beperkt door gebruik te maken van een versleutelde datapayload, al dan niet bovenop de notification message. Als een medewerker beschikt over Unified Push, een alternatieve pushinfrastructuur voor Android, kan de app hiervan ook gebruikmaken en terugvallen op Google als dit niet beschikbaar is.

## 14.2 Proportionaliteit

Om de proportionaliteit van de verwerkingsactiviteiten te beoordelen, dient te worden afgewogen of de ingrijpendheid van de activiteiten evenredig is aan de doeleinden van de activiteiten. Bij de beoordeling van de ingrijpendheid dienen de (privacy)belangen van de betrokkenen in aanmerking te worden genomen. Om deze afweging te structureren, worden vier van de beginselen uit artikel 5 van de AVG gebruikt.

### 14.2.1 Rechtmatigheid, behoorlijkheid en transparantie

Rechtmatigheid betekent dat aan alle wettelijke voorwaarden voor gegevensverwerking wordt voldaan. De instellingen hebben hun eigen rechtsgrondslagen en HR2day beschikt over verwerkersovereenkomsten. Voor subverwerker SignRequest zijn er echter ook veel gegevensdoorgiften die lijken plaats te vinden en die niet zijn verantwoord in de (sub)verwerkersovereenkomst. Bovendien kunnen instellingen, als HR2day en Salesforce verdere verwerkingsactiviteiten uitvoeren, niet aantonen dat zij voldoen aan de vereisten voor verenigbare verdere verwerking op grond van artikel 6 lid 4 AVG. Er zijn ook aanvullende ontvangers die mogelijk als subverwerkers moeten worden gekwalificeerd, waarvoor geen subverwerkersovereenkomsten beschikbaar zijn.

Het transparantiebeginsel waarborgt niet alleen dat toestemming geïnformeerd moet zijn, maar ook dat volledige transparantie over gegevenspraktijken en rechten wordt geboden aan gebruikers. Vanwege het gebrek aan informatie over specifiek de gegevensverwerkingspraktijken van Salesforce met betrekking tot gegevens van HR2day-gebruikers, kunnen HR2day en instellingen niet aan deze eis voldoen. Er bestaat ook onduidelijkheid over de privacyverklaring van HR2day en de verwerking voor eigen doeleinden. Ten slotte veroorzaakt het ontbreken van logging en monitoring van welke informatie een beheerder heeft geraadpleegd bij gebruik van de proxy-loginfunctionaliteit een gebrek aan transparantie.

Behoorlijkheid is een overkoepelend beginsel dat vereist dat persoonsgegevens niet worden verwerkt op een manier die nadelig, discriminerend, onverwacht of misleidend is voor de betrokkene.[89] Vanwege het gebrek aan transparantie kan niet worden beoordeeld of eventuele verdere verwerking eerlijk is ten opzichte van betrokkenen en aansluit bij hun redelijke verwachtingen over de (metadata van de) verwerking van hun HRM- en salarisgegevens.

Concluderend kunnen instellingen, zonder te kunnen uitsluiten dat HR2day en Salesforce persoonsgegevens verder verwerken voor doeleinden die niet in lijn zijn met de doeleinden van de instellingen, HR2day niet gebruiken op een wijze die in overeenstemming is met het beginsel van rechtmatigheid, behoorlijkheid en transparantie. Er dient ook logging te zijn van de informatie die is geraadpleegd met behulp van de proxy-loginfunctionaliteit.

[89] EDPB Richtsnoeren 4/2019 inzake artikel 25 Gegevensbescherming door ontwerp en door standaardinstellingen, versie 2.0, vastgesteld op 20 oktober 2020, p. 16, URL: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, geraadpleegd op 17 oktober 2025.

### 14.2.2 Dataminimalisatie

De beginselen van dataminimalisatie en privacy by design vereisen dat de verwerking van persoonsgegevens wordt beperkt tot wat noodzakelijk is. De gegevens moeten 'toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt' (artikel 5 lid 1 sub c AVG). Dit betekent dat de verwerkingsverantwoordelijke geen gegevens mag verzamelen en opslaan die niet rechtstreeks verband houden met een legitiem doel. Conform dit beginsel dienen de standaardinstellingen voor gegevensverzameling zodanig te worden ingesteld dat de

gegevensverzameling wordt geminimaliseerd door de meest privacyvriendelijke instellingen te gebruiken.

HR2day biedt veel mogelijkheden om workflows te ontwerpen voor verschillende processen met verschillende typen velden binnen het datamodel, waaronder open tekstvelden. Het is aan de instellingen om ervoor te zorgen dat zij uitsluitend de gegevens verwerken die noodzakelijk zijn voor hun processen en open tekstvelden zodanig gebruiken dat het doel ervan duidelijk is, zodat gebruikers niet worden uitgenodigd meer persoonsgegevens te delen dan noodzakelijk.

Salesforce plaatst veel cookies op HR2day en de doeleinden van sommige ervan zijn beschreven op een manier die het moeilijk maakt te beoordelen of de verzamelde gegevens noodzakelijk zijn voor legitieme doeleinden. Dit leidt tot mogelijke schending van het dataminimalisatiebeginsel. Bovendien betekent het feit dat SURF geen uitputtende lijst heeft ontvangen van de gegevensvelden die Salesforce verzamelt, dat niet kan worden beoordeeld of het dataminimalisatiebeginsel wordt nageleefd. Er is ook een gebrek aan informatie over de anonimiseringspraktijken van Salesforce, met name voor hun logs, waardoor niet kan worden beoordeeld of dit op correcte wijze plaatsvindt met betrekking tot het dataminimalisatiebeginsel.

Ten slotte is het niet mogelijk om de toegang te beperken tot uitsluitend de persoonsgegevens die gebruikers nodig hebben voor de uitvoering van hun taken wanneer de functionaliteit voor verticale rechterovererving is ingeschakeld. Dit betekent dat personen hoger in de hiërarchie toegang hebben tot meer persoonsgegevens dan noodzakelijk. Deze functionaliteit is standaard ingeschakeld en organisaties die HR-functionaliteiten toewijzen aan managers 'in de lijn' dienen deze in te schakelen voor een correcte werking van HR2day.

Concluderend kunnen instellingen hun dataminimalisatiepraktijken grotendeels zelf bepalen met betrekking tot de persoonsgegevens die zij kiezen op te slaan in HR2day. Het kan echter niet worden beoordeeld of het dataminimalisatiebeginsel wordt nageleefd met betrekking tot de verwerking van gebruiksgegevens door Salesforce, vanwege een gebrek aan informatie. De functionaliteit voor verticale rechterovererving zorgt ook voor een dataminimalisatiedilemma voor instellingen.

### 14.2.3 Juistheid

Het juistheidsbeginsel vereist dat de persoonsgegevens nauwkeurig zijn en, waar nodig, worden geactualiseerd. "[A]lle redelijke maatregelen [moeten] worden genomen om persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren" (artikel 5 lid 1 sub d AVG).

HR2day biedt koppelingen om gegevens automatisch te importeren vanuit (werving)systemen, waarmee de nauwkeurigheid van gegevens bij invoer in de applicatie wordt gewaarborgd. Als gegevens in de applicatie desondanks onjuist zijn, biedt HR2day functionaliteiten om deze te corrigeren.

Concluderend zijn er binnen HR2day geen technische of functionele beperkingen gevonden die onderwijsinstellingen verhinderen te voldoen aan het juistheidsbeginsel.

### 14.2.4 Opslagbeperking

Het beginsel van opslagbeperking vereist dat persoonsgegevens uitsluitend worden bewaard zolang noodzakelijk voor het betreffende doel. Gegevens moeten "worden bewaard in een vorm die het mogelijk maakt de betrokkenen te identificeren, en niet langer dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor de persoonsgegevens worden verwerkt" (artikel 5 lid 1 sub e, eerste zin AVG). Dit beginsel vereist dan ook dat persoonsgegevens worden verwijderd zodra zij niet langer noodzakelijk zijn om het door de verwerkingsverantwoordelijke beoogde doel te bereiken.

HR2day biedt instellingen de mogelijkheid hun eigen bewaartermijnen voor klantgegevens af te dwingen via signaallijsten en via de functionaliteit voor het instellen van automatische bewaartermijnen voor documenten.

De bewaartermijnen die HR2day hanteert zoals beschreven in 4.3.10 Logging en 5.8 Back-up zijn in lijn met industriestandaarden.

Salesforce bewaart de gegevens die het als verwerker voor HR2day verwerkt zolang het abonnement op de Salesforce-diensten actief is en HR2day of de instellingen de gegevens niet zelf verwijderen. Na beëindiging van het abonnement bewaart Salesforce de gegevens 120 dagen in inactieve status. Daarna worden de klantgegevens binnen 90 dagen overschreven of verwijderd uit de productieomgeving. De gegevens worden binnen 300 dagen na beëindiging van het abonnement verwijderd uit de back-ups. Hoewel dit redelijk standaard industrietermijnen zijn, dient HR2day instellingen de mogelijkheid te bieden deze gegevens op een eerder tijdstip te verwijderen.

Voor eventuele verdere verwerking door Salesforce is onduidelijk welke bewaartermijnen zij hanteren en of deze in overeenstemming zijn met het beginsel van opslagbeperking.

Concluderend zijn instellingen in staat het beginsel van opslagbeperking na te leven voor gegevens die onder hun en HR2day's beheer vallen. Het kan echter niet worden beoordeeld of dit ook het geval is voor verwerking door Salesforce.

### 14.2.5 Integriteit en vertrouwelijkheid

Persoonsgegevens moeten worden verwerkt op een wijze die een passende beveiliging waarborgt en waarbij zij worden beschermd tegen onder meer onrechtmatige of ongeoorloofde verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging (artikel 5 lid 1 sub f AVG in samenhang met artikel 32 lid 1 en 2 AVG).

**Leestoegangslogging**

Het ontbreken van logging voor gegevenstoegang (leestoegangslogging) vergroot het risico dat niet kan worden vastgesteld of onbevoegden persoonsgegevens hebben ingezien bij een autorisatiefout of incident. Als gevolg hiervan is het bij een potentieel datalek onmogelijk vast

te stellen of, en wiens, persoonsgegevens door onbevoegde gebruikers zijn ingezien. Dit betekent dat instellingen geen adequate en gerichte maatregelen kunnen treffen.[90]

**Autorisatie**

HR2day biedt gedetailleerde autorisatiefunctionaliteiten zoals beschreven in 4.3.9 Beheer van rollen en profielen. Het gebruik van de verticale rechterovererving leidt echter tot een situatie waarbij personen hoog in de hiërarchie zeer brede autorisaties hebben die toegang bieden tot alle persoonsgegevens van alle medewerkers in de verticale lijn onder hen in de hiërarchie, wat hun daadwerkelijke behoeften kan overstijgen. Het gevolg van het uitschakelen van deze functionaliteit is dat de ondersteunende processen/workflows niet kunnen worden gevolgd op de verschillende managementniveaus, wat noodzakelijk is wanneer HR-taken worden toegewezen aan managers 'in de lijn'. Het is ook niet mogelijk de toegang te beperken tot uitsluitend de persoonsgegevens die gebruikers nodig hebben voor de uitvoering van hun taken, wat leidt tot een schending van vertrouwelijkheid en dataminimalisatie wanneer deze functionaliteit is ingeschakeld bij organisaties die HR-taken toewijzen aan managers in de lijn.

**Encryptie**

Voor encryptie steunt HR2day op de encryptiepraktijken van Salesforce. Gegevens zijn versleuteld at rest en in transit conform industriestandaarden. Het beheer van de encryptiesleutels ligt echter bij Salesforce, wat betekent dat HR2day in de praktijk niet kan bepalen wie toegang heeft tot de versleutelde informatie.

**Bijzondere en gevoelige categorieën gegevens**

Omdat de verwerking van gevoelige en bijzondere categorieën gegevens inherent een hoger risiconiveau kent, dienen aanvullende beveiligingsmaatregelen te worden getroffen om een passend beveiligingsniveau te waarborgen. Salesforce biedt aanvullende encryptieopties via zijn Salesforce Shield-dienst, die specifiek is ontworpen om extra bescherming toe te voegen voor gevoelige gegevens en bijzondere categorieën persoonsgegevens.[91] HR2day maakt echter geen gebruik van deze verbeterde encryptieniveaus. Als gevolg hiervan zijn gevoelige gegevens en gegevens van bijzondere categorieën niet aanvullend beschermd met cel-niveau encryptie.

Concluderend beperken het ontbreken van leestoegangslogging, de instellingen van de verticale rechterovererving en het ontbreken van aanvullende encryptieopties voor gevoelige en bijzondere categorieën gegevens instellingen bij het creëren van integriteit en vertrouwelijkheid in hun HR2day-omgeving.

[90] Het is een sectorstandaard om leestoegangslogging te implementeren voor persoonsgegevens in ERP- en HRM-systemen. Zie: Richtlijn Logging en Monitoring, https://sec.surf.nl/asset/template-richtlijn-logging-en-monitoring/?category=richtlijnen, p. 16, geraadpleegd op 2 april 2026.

[91] Hyperforce Security, Privacy and Architecture, https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/misc/hyperforce-security-privacy-and-architecture.pdf, p. 12, geraadpleegd op 17 oktober 2025.

# 15 Rechten van betrokkenen

De AVG kent betrokkenen het recht toe op informatie, inzage, rectificatie en verwijdering, bezwaar tegen profilering, gegevensoverdraagbaarheid en het indienen van een klacht. Het is de verplichting van de verwerkingsverantwoordelijke om informatie te verstrekken en op deze verzoeken naar behoren en tijdig in te gaan. Als de verwerkingsverantwoordelijke een verwerker heeft ingeschakeld, vereist de AVG dat de verwerkersovereenkomst bepaalt dat de verwerker de verwerkingsverantwoordelijke bijstaat bij het voldoen aan verzoeken om uitoefening van rechten van betrokkenen. Dit hoofdstuk beoordeelt of instellingen en HR2day voldoen aan de AVG-vereisten met betrekking tot de rechten van betrokkenen en of betrokkenen deze rechten effectief kunnen uitoefenen.

## 15.1 Recht op informatie

Betrokkenen hebben een recht op informatie (artikelen 12-14 AVG). Dit betekent dat verwerkingsverantwoordelijken hen moeten voorzien van gemakkelijk toegankelijke, begrijpelijke en beknopte informatie in duidelijke taal over, onder andere, hun identiteit als verwerkingsverantwoordelijke, de doeleinden van de gegevensverwerking, de beoogde opslagduur en de rechten van betrokkenen.

In de privacyverklaring van HR2day ontbreekt informatie over de vraag of deze van toepassing is op de HR2day-applicatie en zo ja, welke delen. Hoewel HR2day uiteindelijk alle informatie over cookies heeft verstrekt, is er momenteel geen volledige cookieverklaring voor gebruikers. De rol van Salesforce en de persoonsgegevens die het verwerkt, worden ook niet duidelijk gecommuniceerd.

## 15.2 Recht op inzage

Betrokkenen hebben een fundamenteel recht op inzage in de hen betreffende persoonsgegevens (artikel 15 AVG). Op verzoek dienen verwerkingsverantwoordelijken betrokkenen te informeren of zij persoonsgegevens over hen verwerken (direct, of via een verwerker). Als dat het geval is, dienen zij betrokkenen te voorzien van een kopie van de verwerkte persoonsgegevens, samen met informatie over de doeleinden van de verwerking, ontvangers aan wie de gegevens zijn doorgegeven, de bewaartermijn(en) en informatie over hun verdere rechten als betrokkenen, zoals het indienen van een klacht bij de toezichthoudende autoriteit voor gegevensbescherming.

Als verwerkingsverantwoordelijken dienen instellingen te voldoen aan inzageverzoeken van betrokkenen. HR2day dient instellingen hierbij bij te staan.

De reactie op het inzageverzoek aan HR2day was onvolledig (zie 1.2 Inzageverzoek betrokkenen voor de volledige reactie). HR2day heeft wel de in-applicatiegegevens over de betrokkenen, de inloghistorie en de mutatielogs verstrekt. De verdere logging die HR2day uitvoert conform de door hen verstrekte documentatie ontbrak echter in de DSAR-reactie. Bovendien is geen informatie verstrekt over eventuele (verdere) verwerking door Salesforce

en HR2day, zoals de verwerking van gegevens over het gebruik van de HR2day-dienst. De persoonsgegevens die worden verwerkt via subverwerker Expo en SignRequest ontbraken eveneens.

## 15.3 Recht van bezwaar

Betrokkenen hebben het recht bezwaar te maken tegen verwerking op basis van gerechtvaardigde belangen of publieke taken, alsmede tegen direct marketing (artikel 21 AVG).

Voor zover instellingen verwerkingsactiviteiten uitvoeren op basis van hun gerechtvaardigde belangen, dienen zij het recht van bezwaar te faciliteren. HR2day is verplicht instellingen bij te staan bij het faciliteren van dergelijke bezwaren, voor zover redelijkerwijs mogelijk.

## 15.4 Recht op rectificatie en verwijdering

Betrokkenen hebben het recht onjuiste of verouderde informatie te laten corrigeren, onvolledige informatie te laten aanvullen (artikel 16 AVG), en onder bepaalde omstandigheden persoonsgegevens te laten verwijderen (artikel 17 AVG).

HR2day biedt de mogelijkheid gegevens in de applicatie eenvoudig te corrigeren en te verwijderen. Als onjuiste of onvolledige persoonsgegevens worden verwerkt in logbestanden, is dit het gevolg van een onjuistheid of onvolledigheid in de brongegevens, d.w.z. de persoonsgegevens die zijn geregistreerd bij het aanmaken van het account. Logbestanden registreren van nature de persoonsgegevens zoals deze zijn vastgelegd in de brongegevens. Elk verzoek tot rectificatie van deze gegevens dient dan ook te zijn gericht op de brongegevens, en niet op de gegevens in logbestanden. Verzoeken tot verwijdering van persoonsgegevens in logbestanden zullen doorgaans niet van toepassing zijn, omdat geen van de gronden van artikel 17 lid 1 AVG van toepassing is. Het doel van de verwerking van deze persoonsgegevens is het waarborgen van de beveiliging van persoonsgegevens en de HR2day-omgeving in bredere zin. De persoonsgegevens die zijn vastgelegd in logbestanden blijven noodzakelijk voor dit doel totdat deze logbestanden worden verwijderd conform het toepasselijke bewaarbeleid. Bovendien zou het rectificeren of verwijderen van persoonsgegevens uit logbestanden dit doel ondermijnen en de bescherming van persoonsgegevens van betrokkenen die de AVG vereist in gevaar brengen.

# 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 gevonden tijdens het testen en de analyse en vóórdat mitigerende maatregelen worden genomen. De risico's worden vervolgens geclassificeerd op basis van de kans dat zij zich voordoen en de impact op de rechten en vrijheden van betrokkenen wanneer dat het geval is. Het model dat deze DPIA, gebaseerd op "het Rijksmodel", hanteert, maakt gebruik van de risicocategorieën en het risicomodel van de Britse toezichthoudende autoriteit voor gegevensbescherming, de ICO. De ICO noemt de volgende hoofdcategorieën van risico's:

- onvermogen om rechten uit te oefenen (inclusief maar niet beperkt tot privacyrechten);
- onvermogen om toegang te krijgen tot diensten of mogelijkheden;
- verlies van controle over het gebruik van persoonsgegevens;
- discriminatie;
- identiteitsdiefstal of fraude;
- financieel verlies;
- reputatieschade;
- lichamelijk letsel;
- verlies van vertrouwelijkheid;
- heridentificatie van gepseudonimiseerde gegevens; of
- enig ander significant economisch of maatschappelijk nadeel.

Deze hoofdcategorieën bieden richtsnoeren voor het bepalen van specifieke risico's. Door de aangetroffen risico's te representeren naar 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 ICO als volgt:

**Tabel: ICO Risicomodel**

| | **Onwaarschijnlijk (Remote)** | **Denkbaar (Reasonable possibility)** | **Waarschijnlijk (More likely than not)** |
|---|---|---|---|
| **Ernstige schade (Serious harm)** | Laag risico | Hoog risico | Hoog risico |
| **Enige impact (Some impact)** | Laag risico | Gemiddeld risico | Hoog risico |
| **Minimale impact (Minimal impact)** | Laag risico | Laag risico | Laag risico |
| | **Kans op/Waarschijnlijkheid van schade** | | |

Deze DPIA hanteert de volgende betekenissen voor de "kans op schade" en de "ernst van de impact" bij de beoordeling van de risico's:

| Kans | Betekenis |
|---|---|
| Onwaarschijnlijk (Very small) | Het is onwaarschijnlijk dat dit risico zich voordoet. |
| Denkbaar (Reasonable possibility) | Het is denkbaar dat dit risico zich voordoet. |
| Waarschijnlijk (More likely than not) | Het is waarschijnlijk of zeker dat het risico zich voordoet. |

| Impact | Betekenis |
|---|---|
| Minimale impact | De gevolgen voor de betrokkene hebben weinig of verwaarloosbare impact 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 substantiële impact op de rechten en vrijheden van de betrokkene wanneer het risico zich voordoet. |

# 16 Risico's

## Salesforce-risico's

| 16.1 Verlies van controle en verlies van vertrouwelijkheid door ongeoorloofde toegang via doorgiften aan Salesforce | |
|---|---|
| **Kans** | Onwaarschijnlijk – mits doorgiften zijn vastgelegd in VWO;<br>Waarschijnlijk – als doorgiften niet zijn vastgelegd |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog (als doorgiften niet zijn vastgelegd in VWO) |

HR2day zorgt ervoor dat Salesforce klantgegevens host in datacenters binnen de EER. De doorgiften die plaatsvinden als gevolg van het gebruik van Salesforce als verwerker zijn beschreven in de paragrafen over User Information Replication en Content Delivery Networks (CDN).

Salesforce is een Amerikaans bedrijf en valt daarmee binnen het toepassingsgebied van Amerikaans recht. Zoals beschreven in 9.1.1 Verzoeken van opsporingsautoriteiten is er een kans dat Salesforce wettelijk verplicht wordt persoonsgegevens te verstrekken aan Amerikaanse autoriteiten op grond van Amerikaans recht, zoals de CLOUD Act. Omdat Salesforce het beheer van encryptiesleutels verzorgt, kunnen de betrokken gegevens gedecodeerde persoonsgegevens zijn in klantgegevens, loggegevens en IP-adressen van betrokkenen, alsmede eventuele persoonsgegevens in de gebruiksgegevens van Salesforce. De DPA tussen Salesforce en HR2day verplicht Salesforce HR2day te informeren over en door te sturen van bevelen van derden tot verstrekking van persoonsgegevens, dergelijke bevelen te betwisten en betrokkenen schadeloos te stellen als persoonsgegevens zijn overgedragen – voor zover wettelijk toegestaan. Echter bevat de DPA geen canary clause die Salesforce verplicht een instelling te informeren over haar onvermogen om te voldoen aan haar contractuele verplichtingen als zij een verzoek met een zwijgplicht ontvangt.

Verder verleent Salesforce ondersteuningsdiensten zoals beschreven in 9.1.2 Klantondersteuning en technische operationele ondersteuning en 9.1.3 Technische operationele ondersteuning, wat betekent dat personeel uit vijf derde landen toegang kan krijgen tot klantondersteuningsgegevens en databasetabellen. Er zijn organisatorische en technische maatregelen getroffen om deze toegang te minimaliseren en te waarborgen dat wanneer toegang plaatsvindt, minimale negatieve gevolgen kunnen optreden.

Ten slotte kunnen, zoals beschreven in 9.1.4 User Information Replication en 9.1.5 Content Delivery Networks (CDN), inlogverzoeken worden opgeslagen buiten de EU (hoewel HR2day stelt deze functionaliteit niet te gebruiken) en maakt Salesforce gebruik van een CDN.

Het transparantierapport van Salesforce toont dat het eerder verzoeken heeft ontvangen en gehonoreerd voor zowel inhoudelijke als niet-inhoudelijke gegevens. De beschreven bestaande maatregelen voor de gegevensdoorgiften in combinatie met het bestaan van de bescherming van het Data Privacy Framework (dat ook bescherming biedt voor verdere doorgiften), de BCR-P van Salesforce en de SCC's betekenen echter dat zolang het Data Privacy Framework bestaat, de kans op negatieve gevolgen voor betrokkenen onwaarschijnlijk is. Dit vereist wel dat alle doorgiften

correct zijn vastgelegd in de VWO tussen instellingen en HR2day, zodat deze wettelijke beschermingen van toepassing zijn op de doorgiften. Als ze niet zijn vastgelegd, is de kans op schade waarschijnlijk, omdat deze beschermingen dan niet van toepassing zijn. Wanneer ongeoorloofde toegang of openbaarmaking plaatsvindt, leidt dit tot verlies van controle voor betrokkenen, wat kan leiden tot ernstige schade voor hun rechten en vrijheden. Zo kunnen hun (gevoelige of bijzondere categorieën) persoonsgegevens worden verwerkt voor onbekende doeleinden (zoals surveillance) zonder mogelijkheid tot verhaal. Als zodanig is dit risico momenteel laag voor instellingen die de Salesforce-gegevensdoorgiften hebben vastgelegd, en hoog voor instellingen die dit niet hebben gedaan.

| **16.2 Verlies van controle door gebrek aan transparantie over de verwerking van gebruiksdata voor doeleinden van Salesforce** | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

De privacyverklaring van Salesforce stelt dat Salesforce via logbestanden en andere technologieën informatie kan verzamelen over de apparaten van gebruikers en hun gebruik van de diensten van Salesforce. Deze privacyverklaring is van toepassing op alle diensten van Salesforce, inclusief het platform van HR2day. Het sluit uit dat Salesforce klantgegevens verwerkt voor eigen doeleinden, maar omdat de DPA alleen klantgegevens omvat, laat dit de mogelijkheid open dat Salesforce typen gegevens verwerkt die niet in de DPA zijn opgenomen, zoals loggegevens en gebruiksgegevens. Salesforce stelt de gebruiksgegevens te verwerken op een wijze die het niet mogelijk maakt individuen te identificeren. SURF heeft geen verwerking van persoonsgegevens door Salesforce waargenomen zoals beschreven in de privacyverklaring, omdat SURF om onder andere technische redenen geen toegang heeft tot de verwerking van Salesforce. SURF heeft daarom ook de afwezigheid van deze verwerking niet (technisch) kunnen verifiëren of juridisch kunnen uitsluiten. Het is dus onduidelijk welke persoonsgegevens door Salesforce worden verzameld, voor welke doeleinden, wat de bewaartermijnen zijn en hoe Salesforce pseudonimiserings- en anonimiseringstechnieken toepast. HR2day heeft geen uitputtende lijst van gegevensvelden die Salesforce verzamelt in hun gebruiksgegevens kunnen verstrekken, noch een toelichting op hun anonimiseringstechnieken.

SURF kan niet uitsluiten dat Salesforce de persoonsgegevens van HR2day-gebruikers niet verwerkt op de manieren zoals beschreven in de privacyverklaring, inclusief de daaropvolgende verwerking voor eigen doeleinden, zoals serviceverbetering. Omdat er geen verenigbaarheidstoets is uitgevoerd en eventuele verdere verwerkingsactiviteiten niet zijn opgenomen in de verwerkersovereenkomsten, resulteert de mogelijkheid van deze verdere verwerking in een verlies van controle.

De kans op een verlies van controle is waarschijnlijk, omdat Salesforce – ondanks de beste inspanningen van HR2day om deze informatie te verkrijgen – onvoldoende zekerheid heeft kunnen bieden om de informatie in hun privacyverklaring te weerleggen. Dit veroorzaakt ernstige schade voor betrokkenen, omdat de gegevensverwerking zoals beschreven in de privacyverklaring van Salesforce uitgebreid is, de betrokken gegevens gevoelig of bijzonder kunnen zijn en

instellingen geen controle hebben over de verwerking van deze gegevens. Salesforce neemt ook verwerkingsdoeleinden zoals het trainen van AI-modellen op in zijn privacyverklaring, wat een doel is dat ver verwijderd is van de oorspronkelijke doeleinden van instellingen bij het verwerken van hun HR- en salarisgegevens en niet in lijn is met de redelijke verwachtingen van betrokkenen. Bovendien betekent het gebrek aan transparantie dat instellingen niet kunnen voldoen aan de informatierechten van hun betrokkenen. Daarom is dit een hoog risico.

| **16.3 Onvermogen om rechten van betrokkenen uit te oefenen op persoonsgegevens** | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

De reactie op het inzageverzoek aan HR2day was onvolledig. HR2day heeft wel de in-applicatiegegevens over de betrokkenen, de inloghistorie en de mutatielogs verstrekt. De verdere logging die HR2day uitvoert conform de documentatie die zij hebben verstrekt nadat zij hun DSAR-reactie hadden gegeven, namelijk de event monitoring, de setup audit trail en de email logs, ontbrak in de DSAR-reactie. Bovendien is geen informatie verstrekt over de gebruiksgegevens die Salesforce als subverwerker verwerkt. De persoonsgegevens die worden verwerkt via subverwerkers Expo en SignRequest en mogelijke subverwerkers Google en Apple ontbraken eveneens.

Dit leidt tot het risico dat betrokkenen hun rechten onder de AVG niet effectief kunnen uitoefenen. De kans dat dit zich voordoet is waarschijnlijk, omdat het zich daadwerkelijk heeft voorgedaan. Het niet voldoen aan de deadline voor de DSAR, zelfs voor een deel van de gegevens, resulteert in ernstige schade voor de rechten van de betrokkene, omdat het recht op inzage een fundamenteel recht is. Daarom is dit een hoog risico.

| **16.4 Verlies van controle door gebrek aan transparantie over de verwerking van persoonsgegevens via cookies** | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

HR2day beschikt niet over een cookieverklaring die de cookies documenteert die HR2day en zijn subverwerkers (met name Salesforce) gebruiken voor het verzamelen van persoonsgegevens. Betrokkenen zijn daardoor niet in staat zich te informeren over de verwerking die HR2day en hun subverwerkers via cookies uitvoeren voordat de verwerking begint, en kunnen hun rechten niet uitoefenen.

De kans dat dit zich voordoet is waarschijnlijk, omdat er momenteel geen volledige cookieverklaring is. Dit veroorzaakt ernstige schade voor betrokkenen, omdat zij hun rechten als betrokkene niet kunnen uitoefenen. Daarom is dit een hoog risico.

| 16.5 Verlies van controle doordat registratie vereist is voor subverwerkerswijzigingen van Salesforce | |
|---|---|
| **Kans** | Denkbaar |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

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

Er bestaat een denkbaar dat dit zich voordoet, omdat er geen garantie is dat instellingen worden geïnformeerd over nieuwe subverwerkers. Zonder adequate informatie worden betrokkenen niet in een positie gesteld waarin zij hun rechten als betrokkene effectief kunnen uitoefenen, wat leidt tot een verlies van controle dat ernstige schade veroorzaakt. Het algehele risico is hoog.

### Algemene risico's

| 16.6 Verlies van controle door gebrek aan transparantie over de verwerking van persoonsgegevens voor doeleinden van HR2day | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

De verklaring van HR2day stelt dat HR2day gegevens over gebruikers kan verzamelen en verwerken voor eigen doeleinden, zoals het verbeteren van diensten. De formulering van deze verklaring maakt niet duidelijk of HR2day hiervoor gebruikmaakt van persoonsgegevens die het als verwerker heeft verkregen. Dit gebrek aan duidelijkheid over de verwerking door HR2day belet instellingen hun betrokkenen adequaat te informeren over de verwerking van hun persoonsgegevens en over eventuele verdere verwerking die kan plaatsvinden.

De kans op een verlies van controle is waarschijnlijk, omdat de huidige privacyverklaring de mogelijkheid openhoudt dat HR2day klantgegevens voor eigen doeleinden verwerkt. De verdere verwerking veroorzaakt ernstige schade, omdat onduidelijk is welke persoonsgegevens het betreft en de gegevens gevoelig of bijzonder kunnen zijn. Een doel als "het aanmaken van belangstellingsprofielen voor het promoten van relevante producten en diensten (profilering)" is ook niet in lijn met de oorspronkelijke doeleinden van instellingen en de redelijke verwachtingen van betrokkenen. Daarom is dit een hoog risico.

| 16.7 Verlies van controle over gebruikstevredenheidsdata | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Enige impact |
| **Risicoscore** | Hoog |

HR2day verzamelt gebruikerstevredenheidsgegevens voor serviceverbeteringsdoeleinden via pop-ups. Instellingen kunnen deze functionaliteit niet uitschakelen, hebben geen toegang tot deze gegevens en kunnen niet sturen wat HR2day verzamelt. Deze beoordelingen maken geen deel uit van de verwerkersovereenkomsten met de instellingen en instellingen hebben geen mogelijkheid HR2day instructies te geven over deze verwerking.

De verwerking van gebruikerstevredenheidsgegevens door HR2day voor serviceverbetering leidt tot een onverenigbare verdere verwerking van persoonsgegevens voor eigen serviceverbeteringsdoeleinden van HR2day.

De kans dat dit zich voordoet is waarschijnlijk, omdat het de huidige praktijk van HR2day is. Er is enige impact voor betrokkenen, omdat het feit dat zij geen reden hebben te verwachten dat HR2day hun gegevens verwerkt voor eigen serviceverbetering een verlies van controle veroorzaakt. De betrokken dataset is echter beperkt. Daarom is dit een hoog risico.

| 16.8 Verlies van controle en verlies van vertrouwelijkheid door ongeoorloofde toegang in derde landen | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

Tijdens het technisch onderzoek werden doorgiften buiten de EER aangetroffen in relatie tot subverwerker SignRequest voor het elektronisch ondertekenen van overeenkomsten, subverwerker Expo voor het verzenden van mobiele app-notificaties en Google voor het gebruik van de Google Maps-integratie. De overgedragen gegevens kunnen klantgegevens zijn, maar ook andere gegevens zoals loggegevens. De doorgiften gingen deels naar de VS, waarop het Data Privacy Framework van toepassing is, maar het is onduidelijk of er meer (verdere) doorgiften plaatsvonden.

Omdat deze doorgiften niet wettelijk zijn beschermd in de verwerkersovereenkomsten en er geen andere maatregelen zijn om de betrokken persoonsgegevens te beschermen, is de kans op een verlies van controle waarschijnlijk. Dit geldt met name voor SignRequest, dat heeft aangetoond dat het instellingen niet in staat kan stellen gegevens te verwerken op een wijze die voldoet aan de AVG. De impact op de rechten en vrijheden van betrokkenen als dit plaatsvindt, kan ernstige schade zijn, afhankelijk van het type persoonsgegevens dat wordt verstrekt en de partij aan wie het wordt verstrekt. Daarom is dit een hoog risico.

| 16.9 Verlies van controle over subverwerkers en ontvangers door ontbrekende of onjuiste overeenkomsten | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

HR2day heeft een verwerkersovereenkomst met Expo, maar heeft de bijbehorende hoofddienstverleningsovereenkomst niet aan SURF verstrekt. Er is een dienstverleningsovereenkomst en een subverwerkersovereenkomst met SignRequest, maar SignRequest vereist ook dat gebruikers instemmen met hun eigen privacyverklaring wanneer HR2day-gebruikers worden doorgestuurd naar hun diensten. Dit geeft een tegenstrijdig signaal over de rol van SignRequest. Bovendien zijn er enkele ontvangers waarmee in het geheel geen overeenkomsten zijn gesloten. Dit zijn Google en Apple, die gegevens over betrokkenen verwerken bij gebruik van de HR2day-app en bij gebruik van de Google Maps-integratie. Zij dienen ofwel als subverwerker te worden gekwalificeerd, wat betekent dat HR2day subverwerkersovereenkomsten met hen dient te hebben, ofwel als derde-partij ontvangers die gezamenlijk verwerkingsverantwoordelijken of onafhankelijke verwerkingsverantwoordelijken zijn. In het laatste geval dienen instellingen toestemming te geven voor het verstrekken van hun persoonsgegevens aan deze partijen.

Het gebrek aan documentatie veroorzaakt een gebrek aan transparantie over de gegevens die worden verwerkt door deze partijen en een verlies van controle over deze gegevens. De kans dat dit zich voordoet is waarschijnlijk, omdat de documentatie momenteel ontbreekt. Dit kan ernstige schade veroorzaken voor betrokkenen, omdat het ontbreken van overeenkomsten betekent dat er in het geheel geen controle is over deze gegevens en betrokkenen hun rechten als betrokkene niet kunnen uitoefenen. Daarom is dit een hoog risico.

| 16.10 Verlies van vertrouwelijkheid door het ontbreken van 'leestoegangslogging' | |
|---|---|
| **Kans** | Denkbaar |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

Het ontbreken van logging voor gegevenstoegang (leestoegangslogging) vergroot het risico dat niet kan worden vastgesteld of onbevoegden persoonsgegevens hebben ingezien bij een autorisatiefout of incident. Als gevolg hiervan is het bij een potentieel datalek onmogelijk vast te stellen of, en wiens, persoonsgegevens door onbevoegde gebruikers zijn ingezien. Dit betekent dat instellingen geen adequate en gerichte maatregelen kunnen treffen.

Er is een denkbaar dat deze gevolgen zich voordoen, omdat het ontbreken van leestoegangslogging het moeilijk maakt ongeoorloofd inzien te monitoren en te beperken. Het resultaat is ernstige schade, omdat bijzondere en/of gevoelige persoonsgegevens betrokken kunnen zijn en toegang door partijen zowel binnen als buiten de organisatie kan plaatsvinden. Dit is een hoog risico.

| 16.11 Schending van dataminimalisatie door te brede lijsten voor redenen van verzuim | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

Te brede lijsten voor redenen van verzuim in HR2day vormen een schending van het AVG-beginsel van dataminimalisatie. Dit beginsel vereist dat verzamelde persoonsgegevens toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de specifieke doeleinden waarvoor zij worden verwerkt. De mogelijkheid voor instellingen om eigen categorieën voor ziekte of andere redenen van verzuim te definiëren, leidt tot risico's van buitensporige en onnodige verzameling van gevoelige gegevens. Dit kan resulteren in de verwerking van gezondheids- en andere bijzondere categoriegegevens die verder gaan dan het noodzakelijke minimum, wat de privacy van medewerkers aantast en de kans op oneigenlijk gebruik van gegevens of datalekken vergroot.

De kans dat dit risico zich manifesteert, is sterk afhankelijk van de volwassenheid van het team dat HR2day configureert en beheert, waardoor het waarschijnlijk waarschijnlijk is dat het zich voordoet. De impact kan ernstige schade zijn vanwege de aard van de doeleinden die HR2day vervult bij instellingen. Daarom is dit een hoog risico.

| 16.12 Verlies van controle door open tekstvelden | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

De aanwezigheid van mogelijk talrijke open tekstvelden in HR2day, hoewel deze vaak correct zijn gelabeld met beoogde doeleinden, vormt een risico van verlies van controle over persoonsgegevens. Niet alle methoden van veldvalidatie zijn geïmplementeerd, wat kan leiden tot inconsistente of onnauwkeurige gegevensinvoer. Instellingen/klanten kunnen ook nieuwe tekstvelden aanmaken zonder passende doeleinden of adequate labeling toe te voegen, waardoor het risico op ongecontroleerde gegevensverzameling en -verwerking toeneemt. Vanuit privacyperspectief 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 het dataminimalisatiebeginsel wordt geschonden.

De kans dat dit zich voordoet is waarschijnlijk, omdat dit sterk afhankelijk is van de volwassenheid van het team 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 nauwkeurigheid door handmatige registratie van persoonsgegevens | |
|---|---|
| **Kans** | Waarschijnlijk |

| | |
|---|---|
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

De mogelijkheid van handmatige registratie en bewerking van persoonsgegevens in HR2day vormt een risico van gegevensonnauwkeurigheid als gevolg van menselijke fouten. Managers en HR-medewerkers kunnen persoonlijke gegevens zoals arbeidsrelaties, salarissen, verlofregistraties en gebruikersinformatie direct invoeren en wijzigen. Het ontbreken van geautomatiseerde validatie of standaardcontroles bij handmatige gegevensinvoer vergroot de kans op het vastleggen van onjuiste of verouderde informatie. Dit kan leiden tot onbedoelde gevolgen zoals het delen van informatie met onbevoegde partijen, financiële discrepanties en het ten onrechte weigeren van verlof aan medewerkers. Deze situatie onderstreept het belang van het implementeren van corrigerende controles zoals invoervalidatie, auditsporen en periodieke gegevensbeoordelingen ter verbetering van de nauwkeurigheid van gegevens en ter vermindering van privacyrisico's. Uiteindelijk beschermt een hoge gegevenskwaliteit niet alleen de privacy van individuen, maar ook de integriteit en betrouwbaarheid van HR-operaties.

De kans dat deze onnauwkeurigheden zich voordoen, wordt als waarschijnlijk beoordeeld, omdat het risico afhankelijk is van de volwassenheid van het team dat HR2day configureert en beheert in combinatie met het ontbreken van huidige mitigerende maatregelen. Zonder in het systeem geïntegreerde mechanismen voor foutdetectie of -correctie kunnen fouten onopgemerkt blijven en zich verspreiden door gerelateerde processen. Omdat deze fouten directe invloed hebben op de rechten en aanspraken van individuen met tastbare en zinvolle gevolgen, kan de impact voor betrokkenen ernstige schade zijn. Vanwege de ernstige impact en de redelijke kans is dit een hoog risico.

| **16.14 Verlies van controle over bewaartermijnen door gebrek aan automatisering** | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

HR2day beschikt momenteel niet over geautomatiseerde functionaliteit om persoonsgegevens te verwijderen zodra bewaartermijnen verstrijken en kan geen waarschuwingen genereren wanneer dergelijke termijnen eindigen. Onderscheid tussen categorieën persoonsgegevens met verschillende bewaaroverwegingen is ook niet gesystematiseerd. De huidige aanpak steunt op periodieke handmatige verwerking van signaallijsten, die waarschijnlijk inconsistent worden beheerd met uitgebreide intervallen tussen verwijderingsacties. Dit leidt tot een aanzienlijk risico dat persoonsgegevens langer worden opgeslagen dan noodzakelijk, waarmee de dataminimalisatieprincipes worden geschonden en er verlies van individuele controle en vertrouwelijkheid optreedt.

De kans dat dit risico zich manifesteert is waarschijnlijk vanwege de afhankelijkheid van handmatige processen die kwetsbaar zijn voor menselijke fouten en nalatigheid. Dit kan ernstige schade veroorzaken, omdat dit vraagstuk van invloed is op het beginsel van opslagbeperking voor

alle persoonsgegevens beheerd in HR2day, inclusief bijzondere categorieën gevoelige gegevens. Daarom is dit een hoog risico.

| 16.15 Verlies van vertrouwelijkheid door de standaardinstelling voor verticale overerving van rechten | |
|---|---|
| **Kans** | Denkbaar |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

De standaardinstelling voor verticale rechterovererving in het systeem leidt tot een conflict met het door de AVG vereiste dataminimalisatiebeginsel. Verticale overerving stelt rechten in staat automatisch door organisatielagen omhoog te worden doorgegeven, wat kan resulteren in bredere toegang dan noodzakelijk tot persoonsgegevens. Hoewel het uitschakelen van deze overerving de privacybescherming zou verbeteren door de toegang te beperken tot uitsluitend bevoegde personen, leidt dit in sommige gevallen ook tot operationele uitdagingen voor organisaties die HR-taken toewijzen aan managers 'in de lijn'. Deze situatie stelt een aanzienlijk risico van verlies van vertrouwelijkheid bloot, omdat buitensporig overgeërfde toegangsrechten gebruikers in staat kunnen stellen persoonsgegevens in te zien of te beheren die buiten hun legitieme reikwijdte vallen. Om in lijn te zijn met het dataminimalisatiebeginsel dient het systeem gedetailleerde toegangscontrole mogelijk te maken die de beperking van de toegang van groepen op passende wijze ondersteunt, terwijl de noodzakelijke functionele workflows worden gehandhaafd.

De kans dat dit risico zich manifesteert is redelijk. Hoewel HR2day instellingen informeert over de optie om het uit te schakelen, is de instelling voor verticale rechterovererving standaard ingeschakeld. Instellingen die HR-taken toewijzen aan managers in de lijn, dienen de verticale rechterovererving in te schakelen zodat zij hun taken kunnen uitvoeren en realiseren zich mogelijk de impact hiervan niet, waardoor zij niet de juiste maatregelen treffen om schade voor betrokkenen te voorkomen. De impact is ernstig, omdat buitensporig overgeërfde toegangsrechten gebruikers in staat kunnen stellen persoonsgegevens in te zien of te beheren, inclusief gevoelige en bijzondere categorieën persoonsgegevens, die buiten hun legitieme reikwijdte vallen. Daarom is dit een hoog risico.

| 16.16 Verlies van controle door gebrek aan beheer van encryptiesleutels | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Ernstige schade |
| **Risicoscore** | Hoog |

Salesforce als subverwerker is verantwoordelijk voor hosting, encryptie, back-up en beheert bovendien de encryptiesleutels die in deze processen worden gebruikt. Hoewel de subverwerker technische en organisatorische maatregelen dient te implementeren om beveiliging te

waarborgen, blijft de uiteindelijke verantwoordelijkheid voor naleving van gegevensbescherming bij de verwerkingsverantwoordelijke liggen.

De delegatie van sleutelbeheer door HR2day aan een subverwerker voegt een extra laag toe waarbij sleutelbeheerproblemen kunnen leiden tot ongeoorloofde ontsleuteling en datalekken. Omdat HR2day zelf niet verantwoordelijk is voor sleutelbeheer of het opslaan van de sleutels, dient de verwerkingsverantwoordelijke via contractuele en auditmechanismen te waarborgen dat de subverwerker robuuste encryptiesleutelbeheerparktijken hanteert, inclusief veilige sleutelopslag, toegangsbeperkingen, rotatiebeleid en incidentmonitoring. Zonder strikte controles en transparantie kan afhankelijkheid van een subverwerker voor sleutelbeheer de beveiligingspositie verzwakken en meldingen bij datalekken bemoeilijken als sleutels worden gecompromitteerd. Het laten opslaan en beheren van encryptiesleutels door HR2day zorgt er ook voor dat Salesforce geen persoonsgegevens kan delen als het bevelen ontvangt van buitenlandse autoriteiten.

Om aan te tonen hoe de gegevens in de HR2day-applicatie zijn versleuteld, heeft HR2day verwezen naar algemene Salesforce-beveiligingscertificeringen en andere Salesforce-documentatie. Deze documentatie beschrijft, verspreid over ten minste vier verschillende documenten[92], de typen encryptie die Salesforce aanbiedt en biedt zekerheid dat klantgegevens en back-ups versleuteld zijn at rest. Ze bieden echter geen gedetailleerd inzicht in hoe encryptie is geïmplementeerd voor Salesforce-diensten in het algemeen (encryptieprotocollen, hoe vaak sleutels worden geroteerd, waar sleutels worden opgeslagen, etc.), en zeker niet voor HR2day specifiek. De enige bekende feiten zijn dat HR2day gebruik maakt van database-encryptie en geen gebruik maakt van Salesforce Shield.

HR2day bevat gevoelige en bijzondere categorieën gegevens, die aanvullende beschermingsmaatregelen vereisen die verder gaan dan standaardwaarborgen, omdat openbaarmaking ervan tot aanzienlijke schade kan leiden. Salesforce zelf adviseert het overwegen van het gebruik van aanvullende Platform Encryption (met cel-niveau encryptie) voor gevoelige gegevens. Cel-niveau encryptie biedt een extra beschermingsniveau zodra de hoofd-encryptiesleutels worden gecompromitteerd.

De kans op een verlies van controle zodra er sprake is van een beveiligingsinbreuk is waarschijnlijk, omdat HR2day volledig afhankelijk is van Salesforce voor het beheer van de encryptiemethoden. De impact is ernstig, omdat dit vraagstuk van invloed is op alle persoonsgegevens beheerd in HR2day, inclusief bijzondere categorieën gevoelige gegevens, waarvoor standaard geen aanvullende maatregelen zijn getroffen. Daarom is dit een hoog risico.

[92] C5 Report for Salesforce Services on Hyperforce; Hyperforce Security, Privacy and Architecture; System and Organization Controls (SOC2) Type 2 for Salesforce Services on Hyperforce; Salesforce Services First Party Storage Encryption Summary.

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

Op het moment van publicatie heeft SURF nog geen conclusie bereikt 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, zijn hieronder beschreven. SURF voert echter nader onderzoek uit naar de impact van deze risico's en het effect van

beschikbare maatregelen op de risico's. Hierover zal op een later tijdstip een publicatie volgen. In de tussentijd kunnen instellingen actie ondernemen op basis van hun eigen beoordelingen.

| **16.17 Verlies van controle over verwerkte persoonsgegevens door het installeren van de mobiele app via een app store van een derde partij** | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Nader te bepalen |
| **Risicoscore** | Nader te bepalen |

Het risico verbonden aan het aanbieden van de HR2day mobiele app via de Apple App Store en de Google Play Store ligt in de automatische koppeling die wordt gecreëerd tussen het app-gebruik en het persoonlijke Apple- of Google-account van de gebruiker. Deze koppeling stelt deze platformaanbieders in staat 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 het functioneren van de app, conflicteert dit met het beginsel van Privacy by Default en resulteert het in een verlies van controle over persoonsgegevens.

De kans dat dit risico zich manifesteert is waarschijnlijk, omdat een verlies van controle zal optreden zodra de app via een app store wordt gedownload. Als gevolg hiervan stromen persoonsgegevens over medewerkers onvermijdelijk naar derden zoals Apple en Google, waardoor mogelijk de vertrouwelijkheid wordt aangetast en het risico voor de rechten en vrijheden van medewerkers toeneemt. Dit leidt tot de mogelijke blootstelling van persoonsgegevens zonder expliciete noodzaak en de betrokkenheid van grote platformaanbieders.

Alternatieven met minder privacyinbreuk dienen te worden overwogen om de gegevens van gebruikers beter te beschermen en naleving van de dataminimalisatievereisten te waarborgen.

| **16.18 Verlies van controle door de verwerking van pushmeldingen door Google en Apple** | |
|---|---|
| **Kans** | Waarschijnlijk |
| **Impact** | Nader te bepalen |
| **Risicoscore** | Nader te bepalen |

Dit is een risico dat in het algemeen van toepassing is op alle applicaties die gebruikmaken van de pushinfrastructuur van Google of Apple.

De mobiele HR2day-app verstuurt pushmeldingen. De pushmeldingen leiden zowel tot de overdracht van metadata als van inhoud naar Google en Apple. De metadata betreft gegevens zoals apparaat-ID's, IP-adressen en mogelijk het Google- of Apple-account van de medewerker. De inhoud betreft de berichten als die inhoud onversleuteld wordt verzonden, zoals noodzakelijkerwijs het geval is bij het "notification messages"-gedeelte van de pushmeldingen. De inhoud van deze berichten is zichtbaar voor en wordt verwerkt door Google en Apple. Omdat het niet noodzakelijk is persoonsgegevens op te nemen in notificaties, vormt het doen hiervan een schending van 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 notification messages dat de inhoud van de berichten systematisch wordt verwerkt door Google. Het is mogelijk om deze verwerking te beperken door gebruik te maken van een versleutelde datapayload, al dan niet bovenop de notification message. Als een medewerker beschikt over Unified Push, een alternatieve pushinfrastructuur voor Android, kan de app hiervan ook gebruikmaken en terugvallen op Google als dit niet beschikbaar is. Bij het ontbreken van beide mitigerende maatregelen voldoet het gebruik van notification messages niet aan de subsidiariteitseis.

De kans op een verlies van controle is waarschijnlijk, omdat notificaties een standaard onderdeel zijn van de HR2day-app en het verlies van controle optreedt zodra Google of Apple de notificatie ontvangt.

# Deel D. Beschrijving van voorgestelde maatregelen

## 17 Maatregelen

Dit hoofdstuk beschrijft de technische, organisatorische en juridische maatregelen die instellingen en HR2day kunnen nemen om de hierboven beschreven risico's te mitigeren. Voor elk risico beschrijft de bovenste helft van de tabel het huidige risico en toont het de risicoscore uit deel C. De onderste helft 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 basisniveau van organisatorische privacyvolwassenheid. De toepasselijkheid en prioritering van zowel risico's als maatregelen zullen echter aanzienlijk variëren, afhankelijk van de huidige proces-, technische en governance-volwassenheidsniveaus van elke instelling. SURF adviseert sterk dat elke instelling die haar gereedheid in twijfel trekt, een zelfevaluatie uitvoert aan de hand van de gepresenteerde risico's en maatregelen, of begeleiding zoekt bij collega-instellingen, SURF en/of MBO Digitaal. Het is van het grootste belang dat elke instelling dit overzicht kritisch evalueert in het licht van haar eigen operationele context en technische infrastructuur.

### Salesforce-risico's

| **Verlies van controle en verlies van vertrouwelijkheid door ongeoorloofde toegang via doorgiften aan Salesforce** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.1** | Toegang tot persoonsgegevens door buitenlandse autoriteiten | Verlies van controle en verlies van vertrouwelijkheid | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | -* | Alle rechtmatige doorgiften opnemen in de VWO tussen instellingen en HR2day. | Onwaar-schijnlijk | Ernstig | Laag risico |
| **Status HR2day-maatregel(en):** De deadline hiervoor is 31-12-2026. | | | | | |

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

| **Verlies van controle door gebrek aan transparantie over de verwerking van gebruiksdata voor doeleinden van Salesforce** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |

| | | | | | |
|---|---|---|---|---|---|
| **16.2** | Gebrek aan transparantie over verdere verwerking voor doeleinden van Salesforce | Verlies van controle | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | VWO bijwerken tussen HR2day en instellingen met: alle categorieën persoonsgegevens, inclusief gebruiksdata indien van toepassing, die HR2day en subverwerkers namens instellingen verwerken; legitieme bedrijfsdoelstellingen waarvoor HR2day en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor HR2day en subverwerkers geen persoonsgegevens mogen verwerken; auditrecht voor instellingen t.a.v. de VWO.<br><br>Opt-out activeren voor het verstrekken van trainingsdata aan de globale modellen bij gebruik van Einstein Search. | VWO bijwerken tussen HR2day en instellingen met: alle categorieën persoonsgegevens, inclusief gebruiksdata indien van toepassing, die HR2day en subverwerkers namens instellingen verwerken; legitieme bedrijfsdoelstellingen waarvoor HR2day en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden waarvoor HR2day en subverwerkers geen persoonsgegevens mogen verwerken; auditrecht voor instellingen t.a.v. de VWO.<br><br>VWO bijwerken tussen HR2day en Salesforce met: alle categorieën persoonsgegevens, inclusief gebruiksdata indien van toepassing, die Salesforce namens instellingen verwerkt; legitieme bedrijfsdoelstellingen waarvoor Salesforce persoonsgegevens mag verwerken en onder welke voorwaarden; doeleinden waarvoor Salesforce geen persoonsgegevens mag | Onwaar-schijnlijk | Ernstig | Laag risico |

| | | | | | |
|---|---|---|---|---|---|
| | | verwerken; auditrecht voor instellingen t.a.v. de VWO. | | | |
| **Status HR2day-maatregel(en):** De deadline hiervoor is 31-12-2026. | | | | | |

| **Onvermogen om rechten van betrokkenen uit te oefenen op persoonsgegevens** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.3** | Onvolledige reactie op inzageverzoek betrokkenen. | Onvermogen om rechten van betrokkenen uit te oefenen op persoonsgegevens | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | | DSAR-beleid verbeteren zodat HR2day volledige toegang kan bieden tot alle persoonsgegevens die zij en hun subverwerkers verwerken. | Onwaar-schijnlijk | Ernstig | Laag risico |
| **Status HR2day-maatregel(en):** HR2day verbetert het eigen DSAR-beleid vóór 1-8-2026. | | | | | |

| **Verlies van controle door gebrek aan transparantie over de verwerking van persoonsgegevens via cookies** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.4** | Onvolledige cookieverklaring/documentatie. | Betrokkenen zijn niet in staat zichzelf te informeren over de verwerking van persoonsgegevens via cookies. | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | | Volledige cookieverklaring verstrekken aan alle gebruikers die HR2day gebruiken. | Onwaar-schijnlijk | Ernstig | Laag risico |
| **Status HR2day-maatregel(en):** HR2day completeert de cookieverklaring vóór 1-8-2026 en neemt de cookieverklaring op in de jaarlijkse kalender. | | | | | |

| Verlies van controle doordat registratie vereist is voor subverwerkerswijzigingen van Salesforce | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.5** | Verplichte registratie voor subverwerkerswijzigingen van Salesforce. | Verlies van controle. | Denk-baar | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | | Een proces inrichten waarbij HR2day Salesforce-subverwerkers aan instellingen communiceert. | Onwaar-schijnlijk | Ernstig | Laag risico |
| **Status HR2day-maatregel(en):** De deadline hiervoor is 31-12-2026 (afhankelijk van de maatregelen voor risico 16.2). | | | | | |

## Algemene risico's

| Verlies van controle door gebrek aan transparantie over de verwerking van persoonsgegevens voor doeleinden van HR2day | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.6** | Gebrek aan transparantie over verdere verwerking voor doeleinden van HR2day | Verlies van controle | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | VWO bijwerken tussen HR2day en instellingen met: alle categorieën persoonsgegevens, inclusief gebruiksdata indien van toepassing, die HR2day en subverwerkers namens instellingen verwerken; legitieme bedrijfsdoelstellingen waarvoor HR2day en subverwerkers persoonsgegevens mogen verwerken en onder welke voorwaarden; doeleinden | VWO bijwerken tussen HR2day en instellingen (zie maatregelen instelling).<br><br>Privacyverklaring HR2day bijwerken. | Onwaar-schijnlijk | Ernstig | Laag risico |

| | | | | | |
|---|---|---|---|---|---|
| | waarvoor HR2day en subverwerkers geen persoonsgegevens mogen verwerken; auditrecht voor instellingen t.a.v. de VWO. | | | | |

**Status HR2day-maatregel(en):** De deadline hiervoor is 31-12-2026.

| **Verlies van controle over gebruikstevredenheidsdata** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.7** | Verzameling van tevredenheidsdata met HR2day als verwerkings-verantwoordelijke voor verdere verwerking. | Verlies van controle. | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | | Deze verwerking opnemen in de VWO met HR2day als verwerker en instellingen zinvolle controle (via transparantie) en keuzemogelijkheden bieden. | Onwaar-schijnlijk | Ernstig | Laag risico |

**Status HR2day-maatregel(en):** HR2day neemt dit op in de VWO vóór 31-12-2026 en biedt instellingen de mogelijkheid om deze functionaliteit uit te schakelen.

| **Verlies van controle en verlies van vertrouwelijkheid door ongeoorloofde toegang in derde landen** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.8** | Ongeoorloofde toegang door partijen in derde landen. | Verlies van controle en verlies van vertrouwelijkheid. | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | SignRequest niet meer gebruiken. | Alle doorgiften identificeren, minimaal naar Expo en Google.<br><br>Rechtmatige doorgiften aan subverwerkers | Onwaar-schijnlijk | Ernstig | Laag risico |

| | | | | | |
|---|---|---|---|---|---|
| | | opnemen in de VWO tussen HR2day en instelling.<br><br>Instellingen informeren over de partijen waarnaar persoonsgegevens worden doorgegeven en waarmee zij rechtstreeks overeenkomsten moeten sluiten.<br><br>Klanten die stoppen met het gebruik van SignRequest in staat stellen een kopie te verkrijgen van de verwerkte persoonsgegevens van hun betrokkenen en deze zo nodig te verwijderen. | | | |
| **Status HR2day-maatregel(en):** De deadline hiervoor is 31-12-2026. | | | | | |

| **Verlies van controle over subverwerkers en ontvangers door ontbrekende of onjuiste overeenkomsten** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.9** | Ontbrekende of onjuiste overeenkomsten tussen HR2day en haar subverwerkers. | Verlies van controle. | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | | Beoordelen of Google en Apple kwalificeren als subverwerkers, gezamenlijke verwerkings-verantwoordelijken of derde-partij ontvangers. | Onwaar-schijnlijk | Ernstig | Laag risico |

| | | | | | |
|---|---|---|---|---|---|
| | | Google en Apple opnemen in de VWO tussen HR2day en instellingen.<br><br>De noodzakelijke overeenkomsten sluiten met Google en Apple. | | | |

**Status HR2day-maatregel(en):** HR2day streeft ernaar vóór 1-8-2026 subverwerkersovereenkomsten te hebben gesloten met alle subverwerkers. De deadline voor overige maatregelen is 31-12-2026.

| **Verlies van vertrouwelijkheid door het ontbreken van 'leestoegangslogging'** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.10** | Ontbreken van 'leestoegangslogging'. | Verlies van vertrouwelijkheid. | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | 'Leestoegangslogging' implementeren op categorieën gevoelige en bijzondere gegevens als minimum.<br><br>Leestoegangslogging implementeren voor activiteiten die beheerders uitvoeren via de proxy-login.<br><br>Breng gebruikers zo snel mogelijk op de hoogte dat er iemand zich voor hen heeft uitgegeven. | 'Leestoegangslogging' inschakelen op categorieën gevoelige en bijzondere gegevens en voor de proxy-loginfunctionaliteit als minimum. | Onwaar-schijnlijk | Ernstig | Laag risico |

**Status HR2day-maatregel(en):** HR2day stelt leestoegangslogging beschikbaar voor instellingen vóór 31-12-2026. Daarnaast start HR2day een werkgroep met instellingen.

| **Schending van dataminimalisatie door te brede lijsten voor redenen van verzuim** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.11** | Te brede (keuze)lijsten voor redenen van verzuim. | Schending van dataminimalisatie. | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |

| | | | | | |
|---|---|---|---|---|---|
| | Alleen keuzelijsten gebruiken voor het verzamelen van informatie over de reden van verzuim van medewerkers, en een vaste set velden voor het verzamelen van nadere informatie over het verzuim.<br><br>De verzuimkeuzelijst en de vaste set velden laten evalueren door de privacyafdeling, om te waarborgen dat deze in lijn zijn met de AVG-vereisten en beschikbare richtlijnen.<br><br>Zorgen dat gebruikers van HR2day goed worden geïnstrueerd en getraind over welke soorten gegevens mogen worden verwerkt over het verzuim van medewerkers. | Instellingen instructies geven over hoe keuzelijsten te gebruiken voor het verzamelen van gevoelige en bijzondere categorieën gegevens. | Onwaar-schijnlijk | Ernstig | Laag risico |
| **Status HR2day-maatregel(en):** HR2day stelt dat dit in de ontwikkelcyclus is opgenomen en heeft laten zien hoe gebruikers worden gewaarschuwd om geen informatie op te nemen over de aard en oorzaak van het verzuim. De deadline voor deze maatregel is 31-12-2026. | | | | | |

| **Verlies van controle door open tekstvelden** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.12** | Open tekstvelden. | Verlies van controle. | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | Alleen open tekstvelden met een duidelijk doel gebruiken.<br><br>Vragen zo formuleren dat duidelijk is welke (gevoelige/bijzondere) persoonsgegevens wel en niet mogen worden opgegeven in een open | Instellingen instructies geven over hoe open tekstvelden te gebruiken op een wijze die de beginselen van dataminimalisatie respecteert.<br><br>Voldoende opties bieden voor | Onwaar-schijnlijk | Ernstig | Laag risico |

| | | | | | |
|---|---|---|---|---|---|
| | tekstveld, en de beschikbare informatiepictogrammen gebruiken.<br><br>Zorgen dat gebruikers van HR2day goed worden geïnstrueerd en getraind over welke soorten gegevens mogen worden verwerkt in open tekstvelden. | veldvalidatie om onnauwkeurige gegevensverwerking te voorkomen. | | | |

**Status HR2day-maatregel(en):** HR2day stelt dat dit in de ontwikkelcyclus is opgenomen. HR2day waarschuwt voor het gebruik van samenvoegvelden met gevoelige gegevens in het scherm voor het instellen van signalering. De deadline voor deze maatregel is 31-12-2026.

| **Gebrek aan nauwkeurigheid door handmatige registratie van persoonsgegevens** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.13** | Handmatige registratie van persoonsgegevens. | Gebrek aan nauwkeurigheid. | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | Invoer waar mogelijk automatiseren, bijvoorbeeld door HR2day te koppelen aan het wervingssysteem.<br><br>Zorgen dat HR-medewerkers goed worden geïnstrueerd en getraind in de procedures van de instelling voor het zorgvuldig registreren van persoonsgegevens. | Voldoende opties bieden voor veldvalidatie om onnauwkeurige gegevensverwerking te voorkomen. | Onwaar-schijnlijk | Ernstig | Laag risico |

**Status HR2day-maatregel(en):** HR2day stelt dat dit in de ontwikkelcyclus is opgenomen en veldvalidatie heeft getoond voor BSN-nummers en IBAN's. De deadline voor deze maatregel is 31-12-2026.

| **Verlies van controle over bewaartermijnen door gebrek aan automatisering** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.14** | Gebrek aan automatisering bij het | Verlies van controle | Waar-schijnlijk | Ernstig | Hoog risico |

| | | | | | |
|---|---|---|---|---|---|
| | afdwingen van bewaartermijnen | | | | |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | Bewaartermijnen voor persoonsgegevens in HR2day bepalen en beheren.<br><br>Zorgen dat de bewaartermijnen worden nageleefd door processen in te richten om deze af te dwingen, bijvoorbeeld door gebruik te maken van de geautomatiseerde bewaartermijnen voor documenten. | Informatie en instructies geven aan instellingen over de procedure voor het verwijderen van gegevens via signaallijsten.<br><br>Instellingen faciliteren bij het afdwingen van hun bewaartermijnen door de opties voor technische configuratie en beheer van bewaartermijnen per groep persoonsgegevens in HR2day te verbeteren. | Onwaar-schijnlijk | Ernstig | Laag risico |
| | **Status HR2day-maatregel(en):** HR2day is in contact met twee instellingen en werkt aan (i) het gewenste granulariteitsniveau van bewaartermijnen (generiek versus per gegevensgroep) en (ii) de mate van uniformiteit tussen instellingen. De deadline voor deze maatregelen is 31-12-2026. | | | | |

| **Verlies van vertrouwelijkheid door de standaardinstelling voor verticale overerving van rechten** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.15** | Verticale overerving van toegangsrechten als standaardinstelling. | Verlies van vertrouwelijkheid. | Denk-baar | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | De verticale rechterovererving uitschakelen, tenzij het gebruik van deze instelling noodzakelijk is.<br><br>Toegang tot persoonsgegevens beperken voor rollen die geen toegang tot deze | Instellingen proactief informeren over de privacyimplicaties van de instelling voor verticale rechterovererving en hen de keuze bieden om deze in of uit te schakelen.<br><br>Samenwerken met instellingen om de opties te verbeteren voor het respecteren van het | Onwaar-schijnlijk | Ernstig | Laag risico |

| | | | | | |
|---|---|---|---|---|---|
| | gegevens nodig hebben voor de uitvoering van hun taken.<br><br>Transparant zijn naar betrokkenen over het gebruik van de instelling voor verticale rechterovererving en wie toegang heeft tot hun gegevens. | dataminimalisatiebeginsel met de instelling voor verticale rechterovererving ingeschakeld, zodat de administratieve last vermindert, OF hen in staat te stellen de noodzakelijke workflows uit te voeren met de instelling uitgeschakeld. | | | |
| **Status HR2day-maatregel(en):** De deadline hiervoor is 31-12-2026. | | | | | |

| **Verlies van controle door gebrek aan beheer van encryptiesleutels** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16.16** | Verwerking van gevoelige en bijzondere categorieën gegevens. | Verlies van vertrouwelijkheid. | Waar-schijnlijk | Ernstig | Hoog risico |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | Beoordelen of cel-niveau encryptie, encryptie met door de klant beheerde sleutels en 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 overige beveiligingsmaatregelen. | Instellingen informeren over de encryptiemethoden die worden gebruikt voor de HR2day-applicatie en het platform, en over de mogelijkheid van aanvullende beveiligingswaarborgen, zoals cel-niveau encryptie en door HR2day beheerde encryptiesleutels.<br><br>Samenwerken met instellingen bij het beoordelen van het noodzakelijke encryptieniveau voor de persoonsgegevens in HR2day, specifiek voor de gevoelige en bijzondere categorieën persoonsgegevens. | Onwaar-schijnlijk | Ernstig | Laag risico |

| | | | | | |
|---|---|---|---|---|---|
| | | Waar instellingen dit noodzakelijk achten, aanvullende beveiligingswaarborgen implementeren, zoals cel-niveau encryptie en door HR2day beheerde encryptiesleutels. | | | |

**Status HR2day-maatregel(en):** HR2day heeft aanvullende beveiligingswaarborgen beschikbaar voor instellingen vóór 31-12-2026. De mogelijkheid voor instellingen om hun eigen encryptiesleutels te beheren bestaat al. Daarnaast start HR2day een werkgroep met instellingen om de gewenste opties te beoordelen.

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

| **Verlies van controle over verwerkte persoonsgegevens door het installeren van de mobiele app via een app store van een derde partij** | | | | | |
|---|---|---|---|---|---|
| **R.** | **Oorzaak** | **Gevolg** | **Kans** | **Impact** | **Risicoscore** |
| **16. 17** | Vereiste om mobiele apps te downloaden via de Google en Apple app stores | Verlies van controle | Waar-schijnlijk | Nader te bepalen | Nader te bepalen |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | Toegang via een mobiele browser op mobiele apparaten mogelijk maken.<br><br>Een proportionaliteits- en subsidiariteitsbeoordeling uitvoeren ten aanzien van het aanbieden van de mobiele app via app stores en 'sideloading', en de resultaten implementeren. | De app beschikbaar stellen als sideload.<br><br>Toegang via een mobiele browser op mobiele apparaten mogelijk maken. | Nader te bepalen | Nader te bepalen | Nader te bepalen |

**Status HR2day-maatregel(en):** HR2day neemt contact op met instellingen over hun wensen in dit verband.

| **Verlies van controle door de verwerking van pushmeldingen door Google en Apple** |
|---|

| R. | Oorzaak | Gevolg | Kans | Impact | Risicoscore |
|---|---|---|---|---|---|
| **16. 18** | Pushmeldingen moeten worden verzonden via Google en Apple. | Verlies van controle | Waar-schijnlijk | Nader te bepalen | Nader te bepalen |
| | **Maatregelen instelling** | **Maatregelen leverancier** | **Kans** | **Impact** | **Risicoscore** |
| | Geen persoonsgegevens opnemen in de berichten die via pushmeldingen worden verzonden.<br><br>Een proportionaliteits- en subsidiariteitsbeoordeling uitvoeren ten aanzien van het verzenden van pushmeldingen via Google en Apple of Unified Push, en de resultaten implementeren. | Optioneel: Unified Push implementeren voor Android-gebruikers. | Nader te bepalen | Nader te bepalen | Nader te bepalen |
| **Status HR2day-maatregel(en):** HR2day neemt geen stappen voor deze optionele maatregel. | | | | | |

# 18 Conclusie

Deze DPIA heeft zestien hoge risico's voor betrokkenen geïdentificeerd en twee risico's waarvoor 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 de inrichting van HR2day. Twee van de risico's houden verband met het gebruik van de mobiele app. Deze twee risico's gelden voor elke app die gebruikmaakt van een app store en pushmeldingen.

Door de maatregelen te implementeren worden alle hoge risico's gemitigeerd en resteert slechts een laag restrisico. Hoewel het niet strikt noodzakelijk is om lage risico's te mitigeren, wordt dit wel aanbevolen.

Voor al deze risico's is een termijn opgenomen voor het implementeren van de maatregelen. Instellingen kunnen HR2day blijven gebruiken. Als de hoge risico's zijn gemitigeerd, is voorafgaande raadpleging van de toezichthoudende autoriteit voor gegevensbescherming niet vereist. SURF zal in 2027 een actualisatie van deze DPIA publiceren met een conclusie over de implementatie van de resterende maatregelen.

# Bijlage 1 Technische analyse

## 1.1 Gebruiksscenario's / Scenario's

### Betrokken actoren

- Manager 1
- Manager 2
- Medewerker 1
- Medewerker 2
- Human Resource Manager

### 1 Nieuwe medewerker (Onboarding)

Actor: HR Manager

1 Nieuwe medewerker aanmaken (door HR manager of Manager)

2 Het persoonlijke informatieformulier invullen (inclusief naam, adres, contactgegevens, noodcontacten)

3 Gevolgen arbeidsongeschiktheid toevoegen in dossier

4 Contract via SignRequest

5 Vereiste documenten uploaden (kopie paspoort/identiteitskaart)

6 Bankgegevens invoeren

7 Een nieuw gebruikersaccount aanmaken (Medewerker 1) en authenticatiegegevens instellen

### 2 Selfservice: interaction centre

Actoren: Medewerker 1

1 Persoonlijke informatie/dossier raadplegen

~~2 Zoek naar persoonlijke informatie (via zoekfunctie)~~

3 Noodcontact toevoegen

4 Loonstrook downloaden

5 Verlofaanvraag indienen

6 Verlofdagen controleren

7 Voorkeurstaal wijzigen

8 Mobiliteitsformulier invullen

9 Declaratie indienen

### 3 Selfservice management: manager interaction centre

Actor: Manager 1

1 Dossier van Medewerker 1 inzien en beoordelen

2 Verlofaanvraag van Medewerker 1 goedkeuren/afwijzen

3 Mobiliteitsformulier van Medewerker 1 goedkeuren

4 Declaratie van Medewerker 1 goedkeuren/afwijzen

### 4 Disciplinaire maatregel

Actoren: Manager 1, Medewerker 1, HR Manager 1

Medewerker 1

1 Feedback geven over collega-medewerker (Medewerker 2)

~~2 Klacht indienen over Medewerker 2.~~

Manager 1

3 Prestatierapport van collega-medewerker (Medewerker 2) beoordelen

4 Medewerker 1 dient een officiële klacht in tegen Medewerker 2 – buiten HR2day

5 Een disciplinaire maatregel verwerken (Medewerker 2)

6 Medewerker 2 overplaatsen naar een andere afdeling

7 Een salarisaanpassing initiëren (Medewerker 2)

HR Manager 1

8 Medewerkerdossier inzien en beoordelen (Medewerker 2)

9 Klacht/bezwaar van medewerker afhandelen (Medewerker 1) – buiten HR2day

10 Een disciplinaire maatregel verwerken (Medewerker 2)

11 Salarisaanpassing verwerken (Medewerker 2)

### 5 Ziekteverzuim

Actor: Manager 1

1 Ziekteverzuim registreren in het systeem (Medewerker 2)

2 Re-integratieproces starten

### 6 Rapportages en exports

Actor: HR Manager 1

1 Rapport verzuimden

2 Rapport arbeidsongeschiktheidsregeling

3 Rapport verlof

4 Rapport exporteren naar PDF

5 Rapport exporteren naar Excel

Actor: Manager 1

6 Rapport verzuimden

7 Rapport arbeidsongeschiktheidsregeling

8 Rapport verlof

9 Rapport exporteren naar PDF

10 Rapport exporteren naar Excel

## 1.2 Inzageverzoek betrokkenen

**Inzageverzoek betrokkenen ingediend door SURF Vendor Compliance**

Beste SurfHBO (Visma),

Ik ben medewerker bij uw bedrijf en ik heb een account op HR2day acceptatieomgeving van uw bedrijf (https://hr2day-883.my.salesforce.com).

Bij deze wil ik, conform artikel 15 van de AVG, een inzage verzoek indienen voor mijn persoonsgegevens. Dit inzageverzoek betreft alle gegevens die naar mij herleidbaar zijn, inclusief, maar niet beperkt tot, de gegevens opgeslagen in HR2day, logbestanden, auditlogs, gebruiksinteracties en technische foutrapportages.

Aanvullend daarop verzoek ik ook:

- de verwerkingsdoeleinden;
- de betrokken categorieën van persoonsgegevens;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
- indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;
- welke mogelijkheden er zijn om mijn persoonsgegevens te rectificeren of te wissen, om bezwaar te maken tegen de verwerking en welke procedure daar dan voor gevolgd moet worden;
- van gegevens die ik niet zelf heb verstrekt, alle beschikbare informatie over de bron van die gegevens;
- het bestaan van geautomatiseerde besluitvorming, met inbegrip van de in artikel 22, leden 1 en 4, bedoelde profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

NB: ik sta bij u geregistreerd onder de onderstaande twee e-mailadressen. Op het SurfHBO adres ontvang ik geen mail, maar op het SURF e-mailadres wel. U kunt dat adres gebruiken om mijn identiteit vast te stellen.

Veel dank en met vriendelijke groet,

##############

Account e-mailadres: ######@#####

Relevante identificatieparameters:

Bijnaam: Gebruiker##############

IP-adres: 62.250.###.###

sr_uuid: ##############################

U kunt mij bereiken op: ###############

Tabel 18-1, inzageverzoek betrokkenen met verwijderde persoonsgegevens.

**Reactie op het inzageverzoek betrokkenen door HR2day**

Geachte #########,

In het EIC vindt u in het personeelsdossier linksboven bij documenten in het mapje DPIA de persoonsgegevens die in HR2day van u geregistreerd zijn voor zover u deze al niet via het EIC kunt zien, zoals de gegevens betreffende uw salaris, reviews, verlof, verzuim, declaraties en documenten in de andere mappen. De overzichten in het mapje DPIA blijven tot en met 1 juni 2025 beschikbaar en zullen wij daarna verwijderen. Tot die tijd kunt u ze inzien en/of downloaden.

Met betrekking tot uw vragen:

De verwerking heeft als doel uitvoering van salarisverwerking, bekwaam en tevreden personeel.

Grondslag hiervoor is een wettelijke verplichting (onder meer aangifteplicht bij de belastingdienst), overeenkomst (arbeidsovereenkomst) en een gerechtvaardigd belang (zorgplicht personeel voor een goede bedrijfsvoering).

De volgende gegevens categorieën worden vastgelegd met doel en grondslag:

| Gegevenscategorie | Doel / grondslag |
|---|---|
| Algemene persoonsgegevens | Benodigd voor interne communicatie, dienstverband en wettelijke verplichtingen |
| Vertrouwelijke persoonsgegevens | Benodigd voor dienstverband en wettelijke verplichtingen |
| Arbeidsrelatiegegevens | Benodigd voor dienstverband en wettelijke verplichtingen |
| Vertrouwelijke arbeidsrelatiegegevens | Benodigd voor dienstverband en wettelijke verplichtingen |
| Verloninggegevens | Benodigd voor salarisbetaling en wettelijke verplichtingen |
| Vertrouwelijke verloninggegevens | Benodigd voor salarisbetaling en wettelijke verplichtingen |
| Verzuimgegevens | Benodigd voor dienstverband en wettelijke verplichtingen |
| Verlofgegevens | Benodigd voor dienstverband |
| Talentmanagementgegevens | Benodigd voor dienstverband |
| Performancemanagementgegevens | Benodigd voor dienstverband |
| Documenten | Persoonsgebonden documenten (uiteenlopende vertrouwelijkheid) |

Er worden alleen gegevens verstrekt aan binnenlandse instanties vanwege wettelijke verplichtingen. Aan internationale instanties worden geen gegevens geleverd.

De instanties aan wie geleverd wordt:

Belastingdienst: algemene persoonsgegevens, arbeidsrelatiegegevens en verloninggegevens.

Pensioenfonds ABP: algemene persoonsgegevens, arbeidsrelatiegegevens en verloninggegevens

Vereniging Hogescholen: anoniem worden persoonsgegevens, arbeidsrelatiegegevens en verloninggegevens geleverd.

Arbodienst Verzuim: alleen in geval van ziekte worden algemene persoonsgegevens, arbeidsrelatiegegevens, verloninggegevens en verzuimgegevens gedeeld.

De bewaartermijnen zijn afhankelijk van welke soort persoonsgegevens:

| Persoonsgegevens | Bewaartermijn |
|---|---|
| arbeidsovereenkomst en wijzigingen daarvan | tot 2 jaar na einde dienstverband (Vrijstellingsbesluit WBP) |
| verslagen van beoordelingsgesprekken | tot 2 jaar na einde dienstverband (Vrijstellingsbesluit WBP) |
| afspraken inzake demotie of promotie | tot 2 jaar na einde dienstverband (Vrijstellingsbesluit WBP) |
| kopie getuigschrift | tot 2 jaar na einde dienstverband (Vrijstellingsbesluit WBP) |
| gegevens over ziekteverzuim | tot 2 jaar na dienstverband, tenzij deze gegevens langer nodig zijn omdat er sprake is van een arbeidsconflict of een geschil over de toekenning van een arbeidsongeschiktheidsuitkering (AP-beleidsregels 'De zieke werknemer') |
| re-integratiedossier na einde dienstverband | niet langer dan 2 jaar na afronding van de re-integratie, tenzij het re-integratiedossier blijvende afspraken bevat: in dat geval is het noodzakelijk om deze afspraken langer te bewaren. (AP-beleidsregels 'De zieke werknemer') |
| gesloten re-integratiedossier | niet langer dan 2 jaar na afronding van de re-integratie; (AP-beleidsregels 'De zieke werknemer') |
| Salarisadministratie | tot 7 jaar na einde dienstverband (Artikel 3.5.2 Handboek Loonheffing 2018) |
| Salarisafspraken | tot 7 jaar na einde dienstverband (Artikel 3.5.2 Handboek Loonheffing 2018) |
| loonbelastingverklaringen | tot 5 jaar na einde dienstverband (Artikel 3.5.2 Handboek Loonheffing 2018) |

| Persoonsgegevens | Bewaartermijn |
|---|---|
| formulieren met gegevens voor loonheffingen | tot 5 jaar na einde dienstverband (Artikel 3.5.2 Handboek Loonheffing 2018) |
| kopie identiteitsbewijs | tot 5 jaar na einde dienstverband (Artikel 3.5.2 Handboek Loonheffing 2018) |

Pas na 7 jaar na ontslag kan dus alles verwijderd worden; tot die tijd zullen wel gedeeltelijk persoonsgegevens en documenten verwijderd worden.

Via het EIC kunt u middels de processen wijziging van persoonsgegevens doorgeven. Mogelijkheid tot wissen is zeer beperkt door de wettelijke verplichtingen en de lange bewaartermijn van gegevens.

Indien u van mening bent dat er gegevens ten onrechte geregistreerd zijn of niet correct die u middels de EIC-processen kunt aanpassen, dan kunt u hierover een email verzenden naar onze HR-manager ######### emailadres ##########. Graag hierbij in detail aangeven welke gegevens niet goed zijn geregistreerd of welke u wilt wissen. Binnen een maand zal zij hierop reageren.

In het mutatieverslag staat wie de gegevens gewijzigd heeft. Het mutatieverslag staat bij de documenten in de map DPIA.

Er worden geen geautomatiseerde besluitvorming genomen zoals profilering.

Mocht u nog vragen en/of opmerkingen hebben dan hoor ik dat graag.

Met vriendelijke groet,

########,

HR Manager

Tabel 18-2, de per e-mail ontvangen reactie op het inzageverzoek betrokkenen, met verwijderde persoonsgegevens.

## 1.3 Eindpunten

Een overzicht van de eindpunten die zijn gebruikt tijdens onze tests. Voor de Salesforce-eindpunten hebben wij de aanduiding opgezocht aan de hand van de verstrekte documentatie.[93]

| Eindpunt | Eigenaar | Beschrijving |
|---|---|---|
| hr2day-883.lightning.force.com | Salesforce | Salesforce Lightning |
| hr2day-883.my.salesforce.com | Salesforce | Salesforce-aanmelding |
| hr2day-883--hr2d.vf.force.com | Salesforce | Salesforce Visualforce |
| static.lightning.force.com | Salesforce | Salesforce Lightning |
| sentry.sr-staging-1.com | SignRequest | Geen informatie |
| SignRequest.com | SignRequest | Website van SignRequest |

| Eindpunt | Eigenaar | Beschrijving |
|---|---|---|
| maps.googleapis.com | Google | Google Maps API, wordt gebruikt ten behoeve van het opzoeken van adressen in de declaratiemodule |
| deu38.sfdc-yzvdd4.salesforce.com | Salesforce | Niet gespecificeerd in documentatie. In documentatie wordt '.salesforce.com' altijd vermeld met subdomein 'my'; [prefix].my.salesforce.com. |
| hr2day-883.file.force.com | Salesforce | Content |
| www.hr2day.com | HR2day website | Het logo van HR2day wordt daar vandaan gelezen voor weergave in documenten. |
| b.static.lightning.force.com | Salesforce | Niet gespecificeerd in documentatie. Geen '.static.' in combinatie met 'lightning.force.com'. |
| www.dropbox.com | SignRequest | Geen informatie |
| 62vqqh6qv58h.statuspage.io | SignRequest | Geen informatie |
| js.stripe.com | SignRequest | Geen informatie |
| www.googletagmanager.com | SignRequest | Geen informatie |
| login.salesforce.com | Salesforce | Hoewel de URL vanzelfsprekend is, staat deze niet in de documentatie. |
| www.gravatar.com | SignRequest | Geen informatie |
| www.google-analytics.com | SignRequest | Geen informatie |
| SignRequest-pro.s3.amazonaws.com | SignRequest | Geen informatie |
| ajax.googleapis.com | Google | Google API's wordt in combinatie gebruikt met Google Maps API. |
| cdn.prod.website-files.com | SignRequest | Geen informatie |
| cdnjs.cloudflare.com | SignRequest | Geen informatie |
| d3e54v103j8qbb.cloudfront.net | SignRequest | Geen informatie |
| assets.website-files.com | SignRequest | Geen informatie |
| fonts.googleapis.com | SignRequest | Geen informatie |
| region1.google-analytics.com | SignRequest | Geen informatie |
| consent.cookiebot.com | SignRequest | Geen informatie |
| imgsct.cookiebot.com | SignRequest | Geen informatie |
| fonts.gstatic.com | SignRequest | Geen informatie |
| m.stripe.network | SignRequest | Geen informatie |

| Eindpunt | Eigenaar | Beschrijving |
|---|---|---|
| m.stripe.com | SignRequest | Geen informatie |
| hr2day-applanding.herokuapp.com | HR2day | HR2day applanding wordt door de HR2day-app gebruikt om te bepalen op welke instantie-URL een gebruiker mag inloggen. |
| hr2day-883.my.site.com | Salesforce | Salesforce Experience Cloud-sites. |
| csp-report.force.com | Salesforce | Niet gespecificeerd in documentatie. |
| hello.myfonts.net | Onbekend | |
| hr2day-html2pdf.herokuapp.com | Salesforce | Server waarop de PDF-engine zich bevindt voor het genereren van documenten naar .pdf |

Tabel 18-3, overzicht van de tijdens de tests aangetroffen eindpunten.

[93]https://help.salesforce.com/s/articleView?id=xcloud.domain_name_url_format_changes_enable_enhanced.htm&type=5

## 1.4 Cookies

### Cookies HR2day

HR2day plaatst meerdere cookies op het apparaat van de gebruiker. Elk van deze cookies heeft een doel voor het opslaan van gegevens.

| Cookienaam | Leeftijd | Beschrijving |
|---|---|---|
| apex__hr2d_MdwSelPic | | Een ja/nee-waarde om te onthouden of een gebruiker foto's van medewerkers wil zien in het scherm voor de arbeidsrelatie van medewerkers (dit is een keuze in de gebruikersinterface) |
| apex__hr2d_MdwSelUD | | Een ja/nee-waarde om te onthouden of een gebruiker medewerkers uit dienst wil zien (dit is een keuze in de gebruikersinterface) |
| apex__hr2d_reg | | Onthoudt het aantal regels dat de gebruiker op het scherm wil zien (dit is een keuze in de gebruikersinterface in veel schermen) |
| apex__hr2d_wg | | Onthoudt het ID van de laatste geselecteerde werkgever (is een vervolgkeuzelijst in de gebruikersinterface). |

Tabel 18-4, cookies gebruikt door HR2day.

### Cookies Salesforce

Salesforce, als het belangrijkste platform dat door HR2day wordt gebruikt om de code te verwerken, plaatst meerdere cookies op het apparaat van de gebruiker. Elk van deze cookies heeft een doel voor het opslaan van gegevens.

| Cookienaam | Leeftijd | Beschrijving | Informatiebron |
|---|---|---|---|
| CookieConsentPolicy | 1 jaar | Gebruikt om de cookietoestemmingsvoorkeuren van eindgebruikers toe te passen die zijn ingesteld door het client-side hulpprogramma. | SF Documentatie |
| LSKey-c$CookieConsentPolicy | 1 jaar | Gebruikt om de cookietoestemmingsvoorkeuren van eindgebruikers toe te passen die zijn ingesteld door ons client-side hulpprogramma. | SF Support |
| oid | 1 jaar | Slaat de laatste ingelogde organisatie op voor het doorsturen van verzoeken. Wordt gebruikt voor het loggen of de cookie aanwezig is in site- en community-verzoeken van gastgebruikers. | SF Support |
| 79eb100099b9a8bf | Sessie | Browser Fingerprint trigger-cookie. Gebruikt om beveiligingsproblemen met sessies te detecteren. | SF Documentatie |
| RSID | Sessie | Sessie-ID en log in als sessie-ID. Cookies gekopieerd naar respons en zorgen ervoor dat de doel-URL correct wordt opgebouwd in een proxysituatie. | SF Documentatie |
| SUCSP | Sessie | Gebruikt wanneer de gebruikersidentiteit die een beheerder aanneemt, via Log In als andere gebruiker, een gebruiker van de Customer Success Portal (CSP) is. | SF Documentatie |
| SUORG | Sessie | Slaat op of u momenteel "SU'd" (Switched User) bent in een ander gebruikersaccount binnen uw eigen org. | SF Support |
| SUPRM | Sessie | Gebruikt wanneer de gebruikersidentiteit die een beheerder aanneemt, via Log In als andere gebruiker, een gebruiker van de Partner Relationship Management (PRM)-portal is. | SF Documentatie |
| clientSrc | Sessie | Gebruikt voor beveiligingsbescherming. | SF Documentatie |
| inst | Sessie | Gebruikt om verzoeken door te sturen naar een instantie wanneer bladwijzers/hardgecodeerde URL's | SF Documentatie |

| Cookienaam | Leeftijd | Beschrijving | Informatiebron |
|---|---|---|---|
| | | verzoeken naar een andere instantie sturen. | |
| sid | Sessie | Sessie-ID gebruikt om Lightning Platform Soap-API en Rest-API gegevensverbindingen te authenticeren voor de huidige gebruiker. | SF Documentatie |
| sid_Client | Sessie | Gebruikt om sessietampering te detecteren en voorkomen. | SF Documentatie |
| __Host-ERIC_PROD-<willekeurig getal> | 1 minuut | Enterprise Request Infrastructure Cookie (ERIC) draagt het CSRF-beveiligingstoken over tussen de server en de client. De naam geeft de servermodus aan (PROD/PRODDEBUG) en een willekeurig getal. Ander token voor elke Lightning-app. | SF Documentatie |
| __Host-ERIC_PRODDEBUG-<willekeurig getal> | | Enterprise Request Infrastructure Cookie (ERIC) draagt het CSRF-beveiligingstoken over tussen de server en de client. De naam geeft de servermodus aan (PROD/PRODDEBUG) en een willekeurig getal. Ander token voor elke Lightning-app. | SF Documentatie |
| autocomplete | 60 dagen | Bepaalt of de aanmeldingspagina de gebruikersnaam van de gebruiker onthoudt. | SF Documentatie |
| com.salesforce.localInfo | 60 dagen | Slaat de landinstelling (taal- en regionale instellingen) op voor aanmeldingspagina's. Na het aanmelden wordt dit bepaald door gebruikersinstellingen. | SF Support |
| disco | Sessie | Volgt de laatste gebruikersaanmelding en actieve sessie om aanmelding te omzeilen (bijv. OAuth immediate flow). | SF Documentatie |
| lloopch_loid | 1 jaar | Bepaalt of de gebruiker naar een specifieke portaalaanmelding of een app-aanmelding wordt gestuurd. | SF Documentatie |
| lloopch_lpid | 1 jaar | Slaat het laatste aanmeldings-Portal ID op. De cookie wordt ingesteld in frontdoor om de gebruiker naar de opgegeven portaalaanmelding of een app-aanmelding te sturen. | SF Support |
| login | 60 dagen | Als de sessie van de gebruiker is verlopen, gebruikt om de | SF Documentatie |

| Cookienaam | Leeftijd | Beschrijving | Informatiebron |
|---|---|---|---|
| | | gebruikersnaam op te halen en in te vullen op de hoofdaanmeldingspagina bij gebruik van de process builder-app. | |
| loginURL | 60 dagen | Slaat de startpagina op voor orgs die niet inloggen via login.salesforce.com | SF Support |
| oinfo | 3 maanden | Volgt de laatste ingelogde org. | SF Documentatie |
| rememberUn | 60 dagen | Volgt het selectievakje Onthoud mij dat de gebruiker heeft geselecteerd om aanmeldingsaanwijzing in te schakelen. | SF Support |
| sdtsvalid | Sessie | Volgt het selectievakje Onthoud mij dat de gebruiker heeft geselecteerd om aanmeldingsaanwijzing in te schakelen. | SF Support |
| setupgtclose | Sessie | Slaat de interactie van de gebruiker op met een rondleiding of productprocedure in de Salesforce Lightning setup-interface. | SF Support |
| sfdc_lv2 | 1 jaar | Slaat apparaatactiveringsgegevens op voor gebruikers. Als dit niet is ingesteld of verlopen, moeten gebruikers hun identiteit verifiëren bij de volgende aanmelding. | SF Support |
| ak_bmsc | 2 uur | Helpt beschermen tegen aanvallen op kwaadaardige websites. Deze cookie is gekoppeld aan Akamai en wordt gebruikt om onderscheid te maken tussen verkeer van mensen en bots. | SF Support |
| bm_sv | 2 uur | Helpt beschermen tegen aanvallen op kwaadaardige websites | SF Support |
| Geo | Sessie | Deze cookie legt de geografische locatie van de gebruiker vast, inclusief continent, land, staat en stad. Cookie is beschikbaar voor het domein static.lightning.force.com. | SF Support |
| 52609e00b7ee307e | Sessie | Browser Fingerprint-cookie. Gebruikt om beveiligingsproblemen met sessies te detecteren. | SF Support |
| embeddedcomponent calloutcookie | Sessie | Dient als vlag-cookie om te bepalen of een bepaalde UI-callout (rondleidingspop-up) gerelateerd aan Analytics embedded components aan de gebruiker moet worden getoond. | SF Support |

| Cookienaam | Leeftijd | Beschrijving | Informatiebron |
|---|---|---|---|
| setupprofileheadergt | Sessie | Cookies die verschillende aspecten van de Guided Tour-functionaliteit beheren, interactieve rondleidingen die zijn ontworpen om nieuwe gebruikers te helpen specifieke functies te begrijpen. | SF Support |
| setupprofileobjectsandtabsgt | Sessie | Volgt de interactie van de gebruiker met een rondleiding gericht op de instellingen voor Objecten en Tabbladen onder gebruikersprofielen. | SF Support |
| unifiedsearchgt | Sessie | Volgt de rondleidingsstatus voor de Unified Search-ervaring | SF Support |

Tabel 18-5 cookies gebruikt door Salesforce, gegevens deels uit cookiedocumentatie Salesforce[94] (SF Documentatie) deels uit feedback van Salesforce-support en via HR2day (SF Support).

[94] https://help.salesforce.com/s/articleView?id=xcloud.platform_cookies.htm&type=5

### Cookies SignRequest

SignRequest, de subverwerker die door HR2day wordt gebruikt voor het afhandelen van het digitaal ondertekenen van documenten, plaatst meerdere cookies op het apparaat van de gebruiker. Elk van deze cookies heeft een doel voor het opslaan van gegevens.

| Cookienaam | Leeftijd | Beschrijving |
|---|---|---|
| _cfuvid | | Geen documentatie |
| csrftoken | | Geen documentatie |
| sessionid | | Geen documentatie |
| sr_user_tags | | Geen documentatie |
| sr_uuid | | Geen documentatie |
| m | | Geen documentatie |

Tabel 18-6, cookies geplaatst door SignRequest.

### Onbekende derde partij-cookies

| Eigenaar | Cookienaam | Leeftijd | Beschrijving |
|---|---|---|---|
| Myfonts.net | __cf_bm | | Geen documentatie |

Tabel 18-7, cookies geplaatst door derde partijen.

## 1.5 Logging datasets

### Inloghistorie

In verwijzing naar 4.3.10.2.

| Veld | Beschrijving |
|---|---|
| Gebruikersnaam | De naam van de gebruiker die heeft ingelogd. |
| Aanmeldtijdstip | Geformatteerde datum en tijd (CET) waarop de aanmelding heeft plaatsgevonden. |
| Bron-IP | IP-adres van waaruit de gebruiker heeft ingelogd; toont proxy/load balancer IP indien van toepassing. |
| Aanmeldtype | Hoe de aanmelding heeft plaatsgevonden, bijv. via het HR2day-aanmeldscherm of SSO. |
| Status | Geeft aan of de aanmelding is geslaagd en redenen voor mislukking indien van toepassing. |
| Browser | Browser die de gebruiker heeft gebruikt om in te loggen. |
| Platform | Platform dat tijdens het aanmelden is gebruikt, bijv. Windows of Mac. |
| Applicatie | Applicatie of interface die is gebruikt om in te loggen bij Salesforce (HR2day). |
| Clientversie | Versie van de clientapplicatie als er meerdere versies bestaan. |
| API-type | Type API dat is gebruikt als de aanmelding via een API-gebruiker heeft plaatsgevonden. |
| API-versie | API-versie die is gebruikt als de aanmelding via een API-gebruiker heeft plaatsgevonden. |
| Aanmeldings-URL | URL waar de aanmelding heeft plaatsgevonden. |
| Omgeving | In welke omgeving de aanmelding heeft plaatsgevonden. |
| TLS-protocol | TLS-protocolversie die is gebruikt tijdens het aanmelden. |
| TLS Cipher Suite | TLS cipher suite die is gebruikt tijdens het aanmelden. |
| Landcode | Landcode van waaruit de aanmelding is geïnitieerd. |
| Land | Land van waaruit de aanmelding is geïnitieerd. |
| Onderverdeling | Provincie of staat van waaruit de aanmelding heeft plaatsgevonden. |
| Stad | Stad van waaruit de aanmelding is geïnitieerd. |
| Postcode | Postcode van waaruit de aanmelding is geïnitieerd. |
| Breedtegraad | Breedtegraadcoördinaat van de aanmeldlocatie. |
| Lengtegraad | Lengtegraadcoördinaat van de aanmeldlocatie. |
| HTTP-methode | HTTP-methode die is gebruikt tijdens het aanmelden. |
| Authenticatiemethode referentie | Geeft aan of/hoe authenticatie is gedelegeerd aan een externe identiteitsprovider. |
| Aanmeld-subtype | Gedetailleerde informatie over de aanmeldmethode, bijv. OAuth of API-gebruik. |

| Veld | Beschrijving |
|---|---|
| Doorgestuurd voor IP | IP-adres van gebruiker als aanmelding via een tussenpersoon zoals proxy of load balancer heeft plaatsgevonden. |

Tabel 18-8, verwerkte persoonsgegevens in inloghistorie-logging.

### Event logging – Aanmelden

In verwijzing naar 4.3.10.3

| Veld | Beschrijving |
|---|---|
| EVENT_TYPE | Dit is hier altijd Login. |
| TIMESTAMP | Toont de aanmeldtijd (tijdzone GMT) in ISO 8601-formaat zonder scheidingstekens, met milliseconden toegevoegd: YYYYMMDDHHmmSSsss. |
| REQUEST_ID | Een uniek Salesforce-ID dat de aanmeldingstransactie identificeert. |
| ORGANIZATION_ID | Een uniek Salesforce-ID dat de Salesforce-omgeving identificeert waarop wordt ingelogd. |
| USER_ID | Een uniek Salesforce-ID dat de gebruiker identificeert die inlogt. |
| RUN_TIME | De hoeveelheid tijd in milliseconden die nodig is om het verzoek te voltooien. |
| CPU_TIME | De hoeveelheid CPU-tijd in milliseconden die nodig is om het verzoek te voltooien. |
| URL | Het adres waarnaar de gebruiker het aanmeldverzoek heeft gestuurd. |
| SESSION_KEY | Het unieke sessie-ID van de gebruiker. |
| LOGIN_KEY | Een unieke tekenreeks die alle gebeurtenissen binnen een gebruikerssessie koppelt, beginnend met aanmelden en eindigend met afmelden of sessievervaldatum. |
| USER_TYPE | Geeft het licentietype weer van de gebruiker die inlogt. Mogelijke waarden: CsOnly, CspLitePortal, CustomerSuccess, Guest, PowerCustomerSuccess, PowerPartner, SelfService, Standard. |
| REQUEST_STATUS | Geeft aan of het aanmelden is geslaagd. Mogelijke waarden: S: geslaagd, F: mislukt, U: ongedefinieerd, A: autorisatiefout, R: omleiding, N: niet gevonden. |
| DB_TOTAL_TIME | De totale tijd in nanoseconden die nodig is voor een databaseronde. |
| LOGIN_TYPE | Toont de methode die is gebruikt om in te loggen. Mogelijke waarden: 7: AppExchange, A: Application, s: |

| Veld | Beschrijving |
|---|---|
| | Certificate-based login, k: Chatter Communities External User, [etc.] |
| BROWSER_TYPE | Toont het type en de versie van de browser die is gebruikt tijdens het aanmelden. |
| API_TYPE | Geeft het type API weer dat is gebruikt tijdens het aanmelden. Mogelijke waarden: D: Apex Class, E: SOAP Enterprise, M: SOAP Metadata, P: SOAP Partner, S: SOAP Apex, T: SOAP Tooling, f: Feed, l: Live Agent, p: SOAP ClientSync. |
| API_VERSION | Geeft de versie weer van de API die is gebruikt tijdens het aanmelden. |
| USER_NAME | De naam van de gebruiker die inlogt. |
| TLS_PROTOCOL | Toont het TLS-protocol dat is gebruikt tijdens het aanmelden. |
| CIPHER_SUITE | Toont de specifieke versleutelingsalgoritmen die zijn gebruikt om de verbinding te beveiligen. |
| LOGIN_URL | Geeft de URL weer waarnaar de gebruiker het aanmeldverzoek heeft gestuurd. |
| AUTHENTICATION_METHOD_REFERENCE | Geeft de gebruikte authenticatiemethode aan (bijv. standaard, SAML, OIDC of meervoudige authenticatie). |
| LOGIN_SUB_TYPE | De flow die is gebruikt voor aanmelden. Mogelijke waarden: authClientCredentials: OAuth Client Credentials, OauthHybridRefreshToken: OAuth Refresh Token for Hybrid Apps, [etc.] |
| AUTHENTICATION_SERVICE_ID | Geeft een unieke identificatiecode weer die verwijst naar de specifieke authenticatiedienst die is gebruikt tijdens het aanmelden. |
| TIMESTAMP_DERIVED | ISO 8601-formaat met scheidingstekens en milliseconden toegevoegd: YYYY-MM-DDTHHmm:SS.sssZ. |
| USER_ID_DERIVED | Het gebruikers-ID van de ingelogde gebruiker, niet hoofdlettergevoelig. |
| CLIENT_IP | Geeft het IP-adres weer van de gebruiker die inlogt. |
| URI_ID_DERIVED | Toont het Salesforce-ID van de URL die het aanmeldverzoek ontvangt. |
| LOGIN_STATUS | Geeft aan of de aanmelding is geslaagd of niet. |
| SOURCE_IP | Het IP-adres van het apparaat dat het aanmeldverzoek heeft ingediend. Kan een proxy- of tussenapparaat zijn. |

| Veld | Beschrijving |
|---|---|
| FORWARDED_FOR_IP | Het oorspronkelijke IP-adres van het apparaat waar de aanmelding vandaan komt. |

Tabel 18-9, verwerkte persoonsgegevens in event logging bij aanmelden.

### Event logging – Afmelden

In verwijzing naar 4.3.10.3

| Veld | Beschrijving |
|---|---|
| EVENT_TYPE | Dit is hier altijd Logout. |
| TIMESTAMP | Toont de afmeldtijd (tijdzone GMT) in ISO 8601-formaat zonder scheidingstekens, met milliseconden toegevoegd: YYYYMMDDHHmmSSsss. |
| REQUEST_ID | Uniek Salesforce-ID dat de afmeldingstransactie identificeert. |
| ORGANIZATION_ID | Uniek Salesforce-ID dat de Salesforce-omgeving identificeert waarvan wordt afgemeld. |
| USER_ID | Uniek Salesforce-ID dat de gebruiker identificeert die afmeldt. |
| USER_TYPE | Toont het type gebruiker dat afmeldt. Mogelijke waarden: A: Geautomatiseerd Proces, b: High Volume Portal, C: Customer Portal User, D: External Who, F: Self-Service, G: Guest, [etc.] |
| SESSION_TYPE | Het sessietype dat werd gebruikt bij het afmelden. Mogelijke waarden: A: API, I: APIOnlyUser, N: ChatterNetworks, [etc.] |
| SESSION_LEVEL | Sessiebeveiligingsniveau tijdens afmelden (waarde 1 betekent standaardsessie, 10 betekent hoog-zekerheidssessie). |
| BROWSER_TYPE | Browser die is gebruikt tijdens het afmelden. |
| PLATFORM_TYPE | Platform gebruikt door de gebruiker. Als de afmelding plaatsvond vanwege een time-out, is de waarde null. |
| RESOLUTION_TYPE | Schermresolutie van de gebruiker op het moment van afmelden. Als de afmelding plaatsvond vanwege een time-out, is de waarde null. |
| APP_TYPE | Het applicatietype dat werd gebruikt tijdens het afmelden. |
| CLIENT_VERSION | De versie van de client die werd gebruikt tijdens het afmelden. |
| API_TYPE | Het type API-verzoek. |
| API_VERSION | De versie van de API die is gebruikt. |
| USER_INITIATED_LOGOUT | Geeft de waarde 1 terug als de gebruiker expliciet heeft afgemeld via de afmeldknop; in alle andere gevallen (time-out, sluiten browser) is de waarde 0. |
| SESSION_KEY | Uniek sessie-ID van de gebruiker. |

| Veld | Beschrijving |
|---|---|
| LOGIN_KEY | Een unieke tekenreeks die alle gebeurtenissen binnen een gebruikerssessie koppelt, beginnend met een aanmeldgebeurtenis en eindigend met een afmeldgebeurtenis of sessievervaldatum. |
| TIMESTAMP_DERIVED | ISO 8601-formaat met scheidingstekens en milliseconden toegevoegd: YYYY-MM-DDTHHmm:SS.sssZ. |
| USER_ID_DERIVED | Gebruikers-ID van de afgemelde gebruiker; in tegenstelling tot USER_ID is dit veld niet hoofdlettergevoelig. |
| CLIENT_IP | IP-adres van de gebruiker die afmeldt. |

Tabel 18-10, alle gegevens verwerkt in event logging type afmelden.

### Event logging – Hostnaam-omleidingen

In verwijzing naar 4.3.10.3

| Veld | Beschrijving |
|---|---|
| EVENT_TYPE | Dit is hier altijd 'HostnameRedirects'. |
| TIMESTAMP | Toont de tijd (tijdzone GMT) van de omleiding in ISO 8601-formaat zonder scheidingstekens, met milliseconden toegevoegd: YYYYMMDDHHmmSSsss. |
| REQUEST_ID | Uniek Salesforce-ID van de omleiding. |
| ORGANIZATION_ID | Een uniek Salesforce-ID dat de Salesforce-omgeving identificeert waar de omleiding plaatsvindt. |
| USER_ID | Een uniek Salesforce-ID dat de gebruiker identificeert die wordt omgeleid. |
| RUN_TIME | Niet gebruikt in de omleiding; daarom altijd 0. |
| CPU_TIME | Niet gebruikt in de omleiding; daarom altijd Null. |
| URL | Niet gebruikt in de omleiding; daarom altijd Null. |
| SESSION_KEY | Niet gebruikt in de omleiding; daarom altijd Null. |
| LOGIN_KEY | Niet gebruikt in de omleiding; daarom altijd Null. |
| MESSAGE | Niet gebruikt in de omleiding; daarom altijd Null. |
| DOMAIN | Niet gebruikt in de omleiding; daarom altijd Null. |
| SOURCE_HOSTNAME | Dit is de hostnaam van waaruit de omleiding afkomstig is. |
| TARGET_HOSTNAME | De hostnaam waarnaar de gebruiker wordt omgeleid. |
| PATH | Het pad van het oorspronkelijke URL-verzoek, tot aan het eerste vraagteken (?). Het pad wordt ook gebruikt in de doel-URL van de omleiding. |
| REDIRECT_REASON | Geeft de reden voor de omleiding aan. Mogelijke waarden: Omgeleid vanwege een hostnaamconflict; Omleiding onderdrukt om Lightning |

| Veld | Beschrijving |
|---|---|
| | Out-integratiefout te voorkomen; Omleiding geblokkeerd omdat omleidingen voor deze hostnaam zijn uitgeschakeld; Omleiding geblokkeerd omdat omleidingen voor de legacy SOURCE_HOSTNAME niet meer worden ondersteund. |
| REDIRECT_IS_BLOCKED | Geeft aan of de omleiding is geslaagd (waarde 0) of geblokkeerd (waarde 1). |
| REFERRER | Het absolute of gedeeltelijke adres van waaruit het verzoek aan de SOURCE_HOSTNAME afkomstig is. |
| ORIGIN | De origine (protocol, hostnaam en poort) die het verzoek aan de SOURCE_HOSTNAME heeft geactiveerd. |
| TIMESTAMP_DERIVED | ISO 8601-formaat met scheidingstekens en milliseconden toegevoegd: YYYY-MM-DDTHHmm:SS.sssZ. |
| USER_ID_DERIVED | Het gebruikers-ID van de omgeleide gebruiker; in tegenstelling tot USER_ID is dit veld niet hoofdlettergevoelig. |
| CLIENT_IP | Geeft het IP-adres weer van de gebruiker die wordt omgeleid. |
| URL_ID_DERIVED | Niet gebruikt in de omleiding; daarom altijd Null. |

Tabel 18-11, event logging type hostnaam-omleidingen.

### Event logging – CSP-schendingen

In verwijzing naar 4.3.10.3

| Veld | Beschrijving |
|---|---|
| EVENT_TYPE | Dit is hier altijd CSPViolation. |
| TIMESTAMP | Toont de tijd (tijdzone GMT) van het verzoek in ISO 8601-formaat zonder scheidingstekens, met milliseconden toegevoegd: YYYYMMDDHHmmSSsss. |
| REQUEST_ID | Uniek Salesforce-ID van de transactie. |
| BLOCKED_URI | De volledige tekenreeks van de geblokkeerde resource. Als het geblokkeerde resource-verzoek een URL gebruikte, is BLOCKED_URI de volledige URL. |
| BLOCKED_URI_DOMAIN | Als BLOCKED_URI een URL is, bevat dit het domein van die URL. |
| DIRECTIVE | De CSP-richtlijn die het resource-verzoek heeft geblokkeerd. Mogelijke waarden: font-src, frame-src, img-src, media-src, style-src, unsafe-eval, unsafe-inline. |
| CONTEXT | CSP-schendingsgebeurtenissen leggen alleen details vast over geblokkeerde resource-verzoeken van Lightning Experience-pagina's. Deze waarde is daarom altijd "Lightning." |
| UNIQUE_ID | Uniek Salesforce-ID van de gebeurtenis. |

| Veld | Beschrijving |
|---|---|
| DISPOSITION | De instructies voor hoe de user agent de CSP-schending heeft afgehandeld op het moment dat deze optrad. Mogelijke waarden: enforce: het verzoek was geblokkeerd; report: het verzoek was niet geblokkeerd maar werd gerapporteerd. |
| SOURCE | De pagina waar de CSP-schending is ontstaan. |
| COLUMN_NUMBER | Het kolomnummer in het document of script waar de schending heeft plaatsgevonden. |
| LINE_NUMBER | Het regelnummer in het document of script waar de schending heeft plaatsgevonden. |
| SOURCE_FILE | De URL van het script waar de schending heeft plaatsgevonden. Als de schending niet in een script heeft plaatsgevonden, is SOURCE_FILE null. |
| RESOURCE_SAMPLE | Een voorbeeld van de resource die de schending heeft veroorzaakt, meestal de eerste 40 tekens of een lege tekenreeks. |
| TIMESTAMP_DERIVED | ISO 8601-formaat met scheidingstekens en milliseconden toegevoegd: YYYY-MM-DDTHHmm:SS.sssZ. |

Tabel 18-12, event logging type CSP-schending.

### Event logging – API totaal gebruik

In verwijzing naar 4.3.10.3

| Veld | Beschrijving |
|---|---|
| EVENT_TYPE | Dit is hier altijd ApiTotalUsage. |
| TIMESTAMP | Toont de tijd (tijdzone GMT) van het API-verzoek in ISO 8601-formaat zonder scheidingstekens, met milliseconden toegevoegd: YYYYMMDDHHmmSSsss. |
| REQUEST_ID | Uniek Salesforce-ID van de transactie. |
| ORGANIZATION_ID | Een uniek Salesforce-ID dat de Salesforce-omgeving identificeert waar het API-verzoek plaatsvindt. |
| USER_ID | Een uniek Salesforce-ID dat de API-gebruiker identificeert die het verzoek indient. |
| API_FAMILY | Het type API dat wordt gebruikt; bijvoorbeeld Rest, Soap of Bulk. |
| API_VERSION | Toont de versie van de API die is gebruikt. |
| API_RESOURCE | De API-methode of resource. |
| CLIENT_NAME | De naam van de client die het API-verzoek heeft ingediend. |
| HTTP_METHOD | De HTTP-methode, bijv. GET. |
| CLIENT_IP | Het IP-adres van de client die Salesforce-services gebruikt. Een intern Salesforce-IP-adres (bijv. een aanmelding via AppExchange) verschijnt als "Salesforce.com IP." |

| Veld | Beschrijving |
|---|---|
| COUNTS_AGAINST_API_LIMIT | Geeft aan of het verzoek meetelt voor de API-limiet (true) of niet (false). |
| CONNECTED_APP_ID | De naam van de verbonden app die het API-verzoek heeft gedaan. |
| ENTITY_NAME | De naam van het Salesforce-object waartoe het API-verzoek toegang heeft geprobeerd te krijgen. |
| STATUS_CODE | De HTTP-antwoordstatuscode voor het verzoek. |
| CONNECTED_APP_NAME | De naam van de verbonden app die het API-verzoek heeft gedaan. |
| USER_NAME | De gebruikersnaam van de API-gebruiker in Salesforce. |
| TIMESTAMP_DERIVED | ISO 8601-formaat met scheidingstekens en milliseconden toegevoegd: YYYY-MM-DDTHHmm:SS.sssZ. |

Tabel 18-13, event logging type API totaal gebruik.

### Event logging – Apex Unexpected Exceptions

In verwijzing naar 4.3.10.3

| Veld | Beschrijving |
|---|---|
| EVENT_TYPE | Dit is hier altijd ApexUnexpectedException. |
| TIMESTAMP | Toont de tijd (tijdzone GMT) van de fout in ISO 8601-formaat zonder scheidingstekens, met milliseconden toegevoegd: YYYYMMDDHHmmSSsss. |
| REQUEST_ID | Uniek Salesforce-ID van de fout. |
| ORGANIZATION_ID | Een uniek Salesforce-ID dat de Salesforce-omgeving identificeert waar de fout is opgetreden. |
| USER_ID | Een uniek Salesforce-ID dat de gebruiker identificeert die de actie uitvoerde waardoor de fout is opgetreden. |
| EXCEPTION_TYPE | Het klasse-type van de fout. |
| EXCEPTION_MESSAGE | De inhoud van het foutbericht. |
| STACK_TRACE | De stacktracering van de fout. |
| EXCEPTION_CATEGORY | De categorie van de fout, die aangeeft of een limiet zoals heapgrootte of CPU-tijd is overschreden. Mogelijke waarden: LimitException: CpuTime, LimitException: HeapSize, LimitException: Queries, LimitException: QueryRows, LimitException: DmlStatements, LimitException: Callouts. |
| TIMESTAMP_DERIVED | ISO 8601-formaat met scheidingstekens en milliseconden toegevoegd: YYYYMMDDHHmmSSsss. |
| USER_ID_DERIVED | Het gebruikers-ID van de ingelogde gebruiker; in tegenstelling tot USER_ID is dit niet hoofdlettergevoelig. |

Tabel 18-14, event logging type Apex Unexpected Exceptions.

### Wijzigingshistorie (Change History Tracing)

In verwijzing naar 4.3.10.4.

| Object | Beschrijving |
|---|---|
| Afdeling | Afdelingsnummer, Startdatum, Bovenliggende afdeling, Einddatum, E-mail, Gedelegeerde manager, Huisnummer, Kostenplaats, Manager, Naam/Code, Beschrijving, Naam ondertekenende afdeling, Ondertekenaar met, Titel ondertekenaar, Stad, Postcode, Telefoon, Straat, Werkgever, en Website |
| Arbeidsrelatie | Begin van arbeidsrelatie, Afdeling, Alleenstaande ouder toeslag, Arbeidsvoorwaardengroep, Auto, Autowaarde, Bank 2 IBAN, Pensioendeelname 1, Deeltijdfactor, Einde van arbeidsrelatie, Functie, Geldig tot, Geldig van, Loonheffingskorting, Rooster, Salaris, Salarisschaal, Trede, Uurloon, en Wijzigingen |
| Arbeidsrelatiewijziging | Begin van arbeidsrelatie, Alleenstaande ouder toeslag, Datum verwerkt, en Toelichting |
| Declaratiecategorie | Arbeidsvoorwaardencluster, Declaratiecategorie, Looncomponentdefinitie, Beschrijving, Procesdefinitie Code, Type, en Variant |
| Declaratiecategorie Runtime | Arbeidsvoorwaardencluster, Looncomponentdefinitie, Beschrijving, Procesdefinitie Code, Type, en Variant |
| Document Signflow Ondertekenaar | Telefoon (niet in gebruik) |
| Kostenplaats | Startdatum, Budgethouder, Dimensie, Einddatum, Gedelegeerde budgethouder, Naam/Code, Beschrijving, Aggregatiekenmerk, en Werkgever |
| LooncompDefinitie | Hoeveelheid, Hoeveelheidsparameter, Te splitsen looncomponent, Code, Eigenaar, Factor, Factorparameter, Basis, Index, Kostenverdeling, Looncomponent, Loonstrookopties, Beschrijving, Opties, Pro rata, Schema, Grootboekcategorisering, Tarief, Tariefparameter, en Type |
| Looncomponent | Hoeveelheid, Rekening, Bankbeschrijving, Naam rekeninghouder, Bank IBAN, Bankrekening, Bedrag, Factor, Geldig tot, Geldig van, Kostenplaats, Kostenplaats Dim2, Kostenplaats Dim3, Looncomponentdefinitie, Naam looncomponent, Referentie, en Tarief |
| Medew/HR gegevens | Bank IBAN, Burgerlijke staat, Indienstdatum, Uitdienstdatum, Privé-e-mail, Huisnummertoevoeging, Huisnummer, Naam, Postbus huisnummertoevoeging, Postbus huisnummer, Postcode, Poststraat, Poststad, Postcode, Straat, Telefoon, Telefoon 2, en Stad |
| Medew/HR gegevens wijziging | Datum verwerkt, Status, en Toelichting |

| Object | Beschrijving |
|---|---|
| MessageInfo | Datum afgewezen, Datum geaccepteerd, Datum verzonden, Laatste controleerpoging, Laatste verzendpoging, en Status |
| Opleidingswijziging | Datum verwerkt |
| Review | Goedkeuring Medewerker 1, Goedkeuring Medewerker 2, en Goedkeuring Medewerker 3 |
| SignRequest | Status |
| Werkgever | Arbeidsvoorwaardencluster, Bank IBAN, E-mail, Financieel admin-ID, Grootboekschema, Jaar, Loonheffingsnummer, Verloning TWK vorig jaar, Pensioenfondsnummer, en Status |

Tabel 18-15, gegevens die standaard worden verwerkt in de Wijzigingshistorie. Houd er rekening mee dat het geselecteerde object maximaal 20 velden kan loggen.

### Debug logging

In verwijzing naar 4.3.10.5

| Term | Beschrijving |
|---|---|
| Uitvoereenheden | De transactie die een gebruiker uitvoert in HR2day. |
| Code-eenheden | Individuele werkeenheid binnen een transactie. Code-eenheden omvatten bijvoorbeeld triggers, validatieregels, webservice-aanroepen, Visualforce-acties op Apex-controllers, etc. |
| Logboekvermeldingen | Logextract met een grote verscheidenheid aan gebeurtenistypen, bijvoorbeeld SQL-query's, gescheiden door een pipe (\|). |
| Tijdstempel | De tijd waarop de gebeurtenis heeft plaatsgevonden, in het formaat UU:mm:ss.SSS. Tussen haakjes staat de waarde in nanoseconden die is verstreken sinds het begin van het verzoek. |
| Gebeurtenisindicator | De gebeurtenis die de debug-logboekvermelding heeft geactiveerd. Dit bevat aanvullende gegevens (code) die zijn vastgelegd bij de gebeurtenis, zoals de methodenaam of het regel- en tekennummer waar de code is uitgevoerd. |
| Cumulatief resourcegebruik | Toont het gecumuleerde verbruik van systeemresources tijdens de uitvoering van code. |
| Cumulatieve profileringsgegevens | Vastgelegd aan het einde van de transactie en bevat informatie over DML-aanroepen, dure query's en dergelijke. |
| API-versie | API-versie die is gebruikt tijdens de transactie. |
| Logboekcategorie | Type informatie dat is vastgelegd. |
| Logboekniveau | De hoeveelheid informatie die is vastgelegd. |

Tabel 18-16, gegevens verwerkt door debug logging.

### Logboek van instellingswijzigingen (Setup Audit Trail)

In verwijzing naar 4.3.10.6

| Veld | Beschrijving |
|---|---|
| Gebruiker | Gebruiker die de wijziging heeft aangebracht |
| Tijdstempel | Tijdstip van de wijziging |
| Type wijziging | Type wijziging (bijv. nieuw veld, workflow aangepast) |
| Details | Details van wat er precies is gewijzigd |
| IP-adres | IP-adres van waaruit de wijziging is aangebracht |
| Sessie-informatie | Sessie-informatie |

Tabel 18-17, gegevens verwerkt door Logboek van instellingswijzigingen.

### E-maillogboek (Email Logs)

In verwijzing naar 4.3.10.7

| Term | Beschrijving |
|---|---|
| Datum/Tijd | Datum/Tijdstip van verzenden/ontvangen van de e-mail |
| Intern bericht-ID | Uniek Salesforce-ID van de e-mail |
| E-mailgebeurtenis | Code van de gebeurtenis. Mogelijke waarden: R – Ontvangst: de e-mail is succesvol ontvangen; D – Bezorging: de e-mail is succesvol verzonden; T – Tijdelijke fout: de bezorging van de e-mail is vertraagd. Salesforce probeert opnieuw te verzenden.; P – Permanente fout: de e-mail kon niet worden bezorgd |
| Ontvanger | E-mailadres van de ontvanger |
| Verzender | Het "Envelope From"-adres dat is gebruikt in het e-mailbericht |
| Externe host | IP-adres van de applicatieserver die de e-mail heeft bezorgd bij de mailserver |
| Overgedragen bytes | Grootte van het e-mailbericht |
| Salesforce.com-gebruiker | Salesforce-ID van de gebruiker die de e-mail heeft verzonden |
| Berichtkoptekst-ID | Berichtkoptekst-ID aan het begin van elke e-mail |
| Aantal pogingen | Aantal pogingen om de e-mail te bezorgen |
| Seconden in wachtrij | Aantal seconden dat de e-mail heeft gewacht voor bezorging |
| Bezorgingsfase | Bezorgingsfase en foutbericht als het verzenden is mislukt |
| Doorstuuradres | Hostnaam van het aangewezen relaysysteem |
| Doorstuurpoort | Poort van het aangewezen relaysysteem |
| Bezorgingsstatusmelding | Per fase een driecijferige responscode die door de mailserver is geretourneerd |

| Term | Beschrijving |
|---|---|
| TLS-versleuteling | Versleuteling gebruikt voor het e-mailbericht |
| TLS geverifieerd | Geeft aan of het e-mailbericht is geverifieerd of niet |
| SPF-status | Authenticatiestatus van het e-mailbericht via het Sender Policy Framework (SPF) |
| Sender ID-status | Authenticatiestatus van de afzender-ID van het e-mailbericht |
| PRA Sender ID-status | Purported Responsible Address-authenticatiestatus van de afzender-ID van het e-mailbericht |
| DomainKeys-status | DomainKeys-status van het e-mailbericht |
| Koptekst Van | Het "Van"-veld in de e-mailkoptekst |
| DKIM-selector | DKIM-selector van het e-mailbericht |
| DKIM-domein | DKIM-domein gekoppeld aan de DKIM-handtekening |
| DKIM geslaagd | Geeft aan of de DKIM-handtekeningkoptekst is opgenomen in de e-mailkopteksten |

Tabel 18-18, gegevens verwerkt in E-maillogboeken.

## 1.6 HR2day App Pushmeldingen

Dit hoofdstuk beschrijft de mogelijke pushmeldingen die worden weergegeven in de HR2day-app.

Op basis van de geselecteerde code volgt hier een gedetailleerde beschrijving van de mogelijke meldingen, inclusief de exacte tekstinhoud en parameters.

### Meldingen voor de medewerker

Hieronder staan de verschillende meldingstypen die een medewerker kan ontvangen met hun exacte tekstinhoud:

### Documentmeldingen

**Nieuwe loonstrook**

- Nederlands: "Er is een nieuwe salarisspecificatie beschikbaar"
- Engels: "A new payslip is available"
- Body: Bestandsnaam van het document
- Parameters: Geen

**Nieuwe jaaropgave**

- Nederlands: "Er is een nieuwe jaaropgave beschikbaar"
- Engels: "A new annual statement is available"
- Body: Naam van het document
- Parameters: Geen

**Nieuw pensioenafschrift**

- Nederlands: "Er is een nieuwe pensioenspecificatie beschikbaar"
- Engels: "A new pension specification is available"
- Body: Naam van het document
- Parameters: Geen

**Nieuwe uitkeringsspecificatie**

- Nederlands: "Er is een nieuwe uitkeringspecificatie beschikbaar"
- Engels: "A new benefit specification is available"
- Body: Naam van het document
- Parameters: Geen

**Nieuwe vergoedingsspecificatie**

- Nederlands: "Er is een nieuwe vergoedingspecificatie beschikbaar"
- Engels: "A new compensation specification is available"
- Body: Naam van het document
- Parameters: Geen

**Nieuw document (algemeen)**

- Nederlands: "Er is een nieuw document toegevoegd aan je digitale dossier"
- Engels: "A new document has been added to your digital file"
- Body Nederlands: "{0} bijlage is toegevoegd aan je digitale dossier"
- Body Engels: "{0} attachment has been added to your digital file"
- Parameters: {0} = Objecttype label (bijv. "Declaratie", "Functioneringsgesprek")

**Nieuw bestand**

- Nederlands: "Er is een nieuw document toegevoegd aan je digitale dossier"
- Engels: "A new document has been added to your digital file"
- Body Nederlands: "\"{0}\" is toegevoegd aan categorie: {1}"
- Body Engels: "\"{0}\" has been added to category: {1}"
- Parameters: {0} = Bestandsnaam, {1} = Documentcategorie

### Declaratiemeldingen

**Declaratie goedgekeurd**

- Nederlands: "Je declaratie is goedgekeurd"
- Engels: "Your declaration has been approved."
- Body Nederlands: "Je declaratie met nr {0} is goedgekeurd."
- Body Engels: "Your declaration with id {0} has been approved."
- Parameters: {0} = Declaratienummer

**Declaratie afgewezen**

- Nederlands: "Je declaratie is afgekeurd"
- Engels: "Your declaration has been denied"
- Body Nederlands: "Reden: {0}"
- Body Engels: "Reason: {0}"
- Parameters: {0} = Reden van afwijzing

**Declaratie verwerkt**

- Nederlands: "Je declaratie is verwerkt"
- Engels: "Your declaration has been processed"
- Body Nederlands: "Je declaratie met nr {0} is verwerkt"
- Body Engels: "Your declaration with id {0} has been processed"
- Parameters: {0} = Declaratienummer

### Verlofbeheer

**Verlof goedgekeurd**

- Nederlands: "Je verlof is goedgekeurd"
- Engels: "Your leave has been approved"
- Body Nederlands: "Je verlofaanvraag voor {0} {1} is goedgekeurd"
- Body Engels: "Your leave requested for {0} {1} has been approved"
- Parameters: {0} = Startdatum, {1} = Einddatum (of lege string bij eendaags verlof)

**Verlof afgewezen**

- Nederlands: "Je verlof is afgekeurd"
- Engels: "Your leave has been denied"
- Body Nederlands: "Je verlofaanvraag voor {0} {1} is NIET goedgekeurd"
- Body Engels: "Your leave request for {0} {1} has NOT been approved"
- Parameters: {0} = Startdatum, {1} = Einddatum (of lege string bij eendaags verlof)

### Prestatieboordelingen

**Beoordeling aangevraagd**

- Nederlands: "Het is tijd voor een {0}"
- Engels: "It is time for a {0}"
- Body Nederlands: "Je bent aan de beurt in het {0} proces"
- Body Engels: "It is your turn in the {0} process"
- Parameters: {0} = Gelokaliseerde beoordelingsstring (bijv. "functioneringsgesprek")

### Procesbeheer

**Procesinstantie goedgekeurd**

- Nederlands: "Je wijziging is goedgekeurd"
- Engels: "Your change has been approved"
- Body: Naam van de procesinstantie
- Parameters: Geen

**Verwerkingsautorisatie afgewezen**

- Nederlands: "Je wijziging is afgewezen"
- Engels: "Your change has been denied"
- Body Nederlands: "Reden: {0}"
- Body Engels: "Reason: {0}"
- Parameters: {0} = Opmerkingen/reden van afwijzing (beperkt tot 255 tekens)

### Algemene meldingen

**Document ondertekenen**

- Nederlands: "Je wordt gevraagd een document te ondertekenen"
- Engels: "You are requested to sign a document"
- Body: Aangepaste tekst (parameter)
- Parameters: Body wordt meegegeven als parameter

**Nieuwe openstaande actie**

- Nederlands: "Er is een nieuwe openstaande actie"
- Engels: "There is a new open action"
- Body: Alerttekst
- Parameters: Geen (body komt uit alert-record)

**Nieuwe mededeling**

- Nederlands: "Er is een nieuwe mededeling"
- Engels: "There is a new announcement"
- Body: Naam van de mededeling
- Parameters: Geen

**Nieuwe vragenlijst**

- Nederlands: "Er is een nieuwe vragenlijst"
- Engels: "There is a new survey"
- Body: Naam van de vragenlijst
- Parameters: Geen

### Meldingen voor de manager

### Verlofaanvragen

**Verlofaanvraag ingediend**

- Onderwerp Nederlands: "Verlofaanvraag"
- Onderwerp Engels: "Leave request"
- Body Nederlands: "Verlofaanvraag van {0} wacht op goedkeuring - Datum: {1} {2}"
- Body Engels: "Leave request by {0} is waiting for approval - Date: {1} {2}"
- Parameters: {0} = Naam van de medewerker, {1} = Startdatum, {2} = Einddatum (met "t/m" prefix, of leeg bij eendaags verlof)
- Trigger: Wanneer verlofstatus wijzigt naar "Ingediend"
- Ontvanger: Approver1 van het verlof

### Algemene wijzigingen (via Process Engine)

**Sjabloon voor alle wijzigingstypen**

- Onderwerp: "{0}" (het type wijziging)
- Body Nederlands: "{0} van {1} wacht op goedkeuring"
- Body Engels: "{0} by {1} is waiting for approval"
- Parameters: {0} = Type wijziging (gelokaliseerd), {1} = Naam van de medewerker

**Specifieke wijzigingstypes**

**Arbeidsrelatiewijziging**

- Nederlands: "Arbeidsrelatiewijziging"
- Engels: "Employment relationship change"
- Trigger: Via ProcessAssignment voor hr2d__ArbeidsrelatieChange__c

**Declaratie (via Process Engine)**

- Nederlands: "Declaratie"
- Engels: "Declaration"
- Trigger: Via ProcessAssignment voor hr2d__Declaration__c

**Medewerkerwijziging**

- Nederlands: "Medewerkerwijziging"
- Engels: "Employee change"
- Trigger: Via ProcessAssignment voor hr2d__EmployeeChange__c

**Looncomponentwijziging**

- Nederlands: "Looncomponentwijziging"
- Engels: "Wage type change"
- Trigger: Via ProcessAssignment voor hr2d__LooncompOutputChange__c

**Kwalificatie**

- Nederlands: "Kwalificatie"
- Engels: "Qualification"
- Trigger: Via ProcessAssignment voor hr2d__Qualification__c

**Verlofregeling opname**

- Nederlands: "Verlofregeling opname"
- Engels: "Leave scheme booking"
- Trigger: Via ProcessAssignment voor hr2d__LeaveSchemeBooking__c

**Opleidingswijziging**

- Nederlands: "Opleidingswijziging"
- Engels: "Education history change"
- Trigger: Via ProcessAssignment voor hr2d__EducationHistoryChange__c

### Declaraties (Oude flow)

**Declaratie ingediend (verouderd)**

- Onderwerp: "Declaratie" (gebruikt CHANGE_SUBMITTED_SUBJECT-sjabloon)
- Body Nederlands: "Declaratie van {0} wacht op goedkeuring"
- Body Engels: "Declaration by {0} is waiting for approval"
- Parameters: {0} = Naam van de medewerker
- Trigger: Wanneer declaratiestatus wijzigt naar "Ingediend" (oude flow, zonder ProcessInstance)
- Ontvanger: Approver_1 van de declaratie

### Opleidingswijzigingen (verouderde flow)

**Opleidingswijziging per goedkeuringsstap**

- Onderwerp: "Opleidingswijziging"
- Body Nederlands: "Opleidingswijziging van {0} wacht op goedkeuring"
- Body Engels: "Education history change by {0} is waiting for approval"
- Parameters: {0} = Naam van de medewerker
- Trigger: Wanneer status wijzigt naar "Ingediend" en er een actieve goedkeuringsstap is
- Ontvangers: Afhankelijk van de stap (Approver1 t/m Approver5)
- Stappen: Ondersteunt tot 5 opeenvolgende goedkeuringsstappen

### Technische details

**Lokalisatie**

- Ondersteunde talen: Nederlands (nl_NL) en Engels (en_US)
- Standaard: Nederlands wordt gebruikt als terugvaloptie voor niet-ondersteunde landinstellingen
- Taalbepaling: Automatisch op basis van de landinstelling van de medewerker

**Parametervervanging**

- Parameters worden vervangen met de methode `String.format()`
- Tijdelijke aanduidingen gebruiken de notatie {0}, {1}, {2} etc.
- Datums worden opgemaakt met de methode `.format()`
- Sommige parameters hebben logica voor eendaags versus meerdaags verlof

# Bijlage 2 Gegevenscategorieën

### Direct identificeerbare gegevens

Dit zijn gegevens die worden gebruikt om een persoon uniek te identificeren (en te authenticeren/autoriseren). Voorbeelden zijn naam (voornaam, achternaam), geboortedatum en -plaats, burgerservicenummer (BSN), paspoort- of identiteitskaartnummer en biometrische gegevens (zoals vingerafdrukken of gezichtsherkenning).

### Contactgegevens

Deze gegevens worden gebruikt om contact op te nemen met een persoon. Voorbeelden zijn: e-mailadres, telefoonnummer (vast en mobiel), postadres en social media-accounts.

### Demografische gegevens

Dit zijn gegevens die de algemene kenmerken van een persoon beschrijven. Voorbeelden zijn leeftijd, geslacht, nationaliteit, burgerlijke staat, opleidingsniveau en beroep of functie.

### Organisatiegegevens

Deze gegevens hebben betrekking op de organisatie waarbij een persoon is aangesloten. Voorbeelden zijn bedrijfsnaam, functietitel, afdeling, werkadres, zakelijk e-mailadres en telefoonnummer.

### Technische gegevens

Deze gegevens hebben betrekking op de technische aspecten van het gebruik van apparaten en diensten. Voorbeelden zijn apparaat-ID's, browsertype en -versie, besturingssysteem, cookiegegevens, logbestanden en gebruiksstatistieken van apps of websites.

### Financiële gegevens

Gegevens die informatie onthullen over iemands financiële situatie.

### Bijzondere categorieën persoonsgegevens

Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakvereniging blijken, en de verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over gezondheid of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Deze gegevens zijn zeer gevoelig en zijn onderworpen aan een aparte interpretatie in de AVG.