Driving innovation together

DPIA HR2day

Application for human resource and payroll management

Author(s)): Sophia Gelpke & Jan Landsaat
Version: 1.0
Date: 12 May 2026

Table of contents

Version history

Version	Date	Summary of changes
0.2	20 May 2025	First draft of part A, shared with HR2day
0.3	24 May 2025	Remarks HR2day (Henk/Marco) incorporated
0.5	17 October 2025	Completely updated Part A after review HR2day and internal review and addition of part B & C
0.66	3 February 2026	Complete concept DPIA with HR2day review on 0.5 incorporated
0.7	3 April 2026	Complete DPIA version with summary, conclusion and HR2day review on 0.66 incorporated
1.0	30 April 2026	Final DPIA version with updates version history, status table and cover sheet included

Cover sheet with HR2day's opinion on the DPIA – 10 April 2026

This cover sheet represents HR2day's vision on the DPIA. Any statements, opinions, or representations appearing in the cover sheet or listed as part of HR2day's vision are attributed solely to HR2day and do not necessarily reflect the views, findings, or conclusions of SURF.

Oplegger HR2day B.V. bij de referentie-DPIA HR2day

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

Summary

This report is a Data Protection Impact Assessment (hereinafter: DPIA) on the use of the SaaS application HR2day by Dutch educational institutions (hereinafter: institutions), offered by HR2day B.V. (hereinafter: HR2day). This DPIA is a reference DPIA, carried out by sector organisation SURF, which provides institutions with a general framework for assessing data protection risks within HR2day.

About the service
HR2day is an all-round HRM and payroll system, that consists of different modules and supports the entire employee journey from onboarding to offboarding and everything in between. It provides default processes that can be tailored for the use of individual institutions and is used by both vocational colleges and universities for applied sciences. As a cloud-based SaaS application, HR2day is built to run natively on the Salesforce platform, using core Salesforce technologies/services to deliver a scalable HR experience.

Scope
SURF performed both legal research and technical research to identify general data protection risks that result from the data processing activities carried out by institutions in HR2day. The tested modules are:

- Personnel and payroll administration
- Self-service (ESS/MSS)
- Leave
- Absences
- Expense claims
- Document management
- Reports
- Digital signature
- HR analytics
- Employee feedback
- “Arbokoppeling” (API)

Additionally, SURF assessed the mobile application HR2day+.

As this is a reference DPIA, it does not contain an assessment of the lawfulness of specific processing activities, nor risks that are specific to individual institutions. Rather, a more general assessment is made based on the envisioned use of HR2day by institutions. Institutions wishing to use HR2day can use this DPIA as a starting point, but must supplement, expand and/or adapt it based on the specific context in which they intend to use HR2day.

Methodology
SURF used the following methods to perform the assessment:

- Desk research and legal review on HR2day’s contracts, certifications and other documentation.

- Questionnaires to the representatives of HR2day.
- Technical investigation in the in-browser application, carried out in a testing environment HR2day created for SURF, including use of a specialised monitoring tool (man-in-the-middle proxy).
- Data Subject Access Requests, filed after technical investigation was performed.
- Reviews by HR2day and SURF.

Outcome: 16 high risks and 2 risks to be determined
This DPIA has identified sixteen high risks for data subjects and two risks for which the risk level is to be determined. Five of the high risks are related to the use of Salesforce as provider of the platform HR2day runs on. Eleven of the high risks are general risks, caused either by the way institutions (are likely to) use HR2day or by the design of HR2day. Two of the risks are related to use of the mobile app. These two risks exist for any app using app store and push notifications. Since SURF is doing an additional investigation into the impact of these risks, the risk level will be determined at a later time.

Implementing these measures will mitigate all high risks, leaving only low residual risks. Although it is not strictly necessary to mitigate low risks, it is recommended.

All of these risks have a timeline for implementing the measures. Therefore, institutions can continue using HR2day. If the high risks are mitigated, no prior consultation with the data protection authority is required. SURF will publish an update on this DPIA with a conclusion on the implementation of the remaining measures in 2027.

An overview of all identified risks and proposed measures is presented in the table below. The status of the measures for HR2day to take is reflected in the right-hand column.

#	Risk	Measures institution	Measures HR2day	Status HR2day measure(s)
Risks related to Salesforce platform				
16.1	Loss of control and loss of confidentiality due to unauthorised access throughby transfers to Salesforce	Include all lawful transfers in DPA	Include all lawful transfers in DPA	The deadline for this is 31-12-2026.
16.2	Loss of control due to a lack of transparency about processing usage data for	Update DPA between HR2day and institutions with: all categories of personal data,	Update DPA between HR2day and institutions with: all categories of personal data, including usage data	The deadline for this is 31-12-2026.

	purposes Salesforce	including usage data if applicable, HR2day and subprocessors process on behalf of institutions; legitimate business objectives HR2day and subprocessors are allowed to process personal data for and under which conditions; purposes HR2day and subprocessors are not allowed to process personal data for; audit right for institutions with regard to the DPA.	if applicable, HR2day and subprocessors process on behalf of institutions; legitimate business objectives HR2day and subprocessors are allowed to process personal data for and under which conditions; purposes HR2day and subprocessors are not allowed to process personal data for; audit right for institutions with regard to the DPA.	
			Update DPA between HR2day and Salesforce with: all categories of personal data, including usage data if applicable, Salesforce processes on behalf of institutions; legitimate business objectives Salesforce is allowed to process personal data for and under which conditions; purposes Salesforce is not allowed to process personal data for; audit right for institutions with regard to the DPA.	The deadline for this is 31-12-2026.
16.3	Inability to exercise data subject access rights to personal data		Improve DSAR policy so HR2day is able to provide full access to all personal data they and their	HR2day will improve their own DSAR policy by 1-8-2026.

			subprocessors process.	Access to possible Salesforce personal data is dependant on implementing the measures for risk 16.2.
16.4	Loss of control due to lack of transparency about processing of personal data through cookies		Provide complete cookie statement to all users who use HR2day.	HR2day will complete the cookie statement by 1-8-2026 and incorporate the cookie statement into their yearly calendar.
16.5	Loss of control due to having to register for subprocessor updates Salesforce		Implement a process where HR2day communicates Salesforce subprocessors to institutions.	The deadline for this is 31-12-2026 (dependant on measures for risk 16.2).
General risks				
16.6	Loss of control due to a lack of transparancy about processing personal data for purposes HR2day	Update DPA between HR2day and institutions with: all categories of personal data, including usage data if applicable, HR2day and subprocessors process on behalf of institutions; legitimate business objectives HR2day and subprocessors are allowed to process personal data for and under which conditions; purposes HR2day	Update DPA between HR2day and institutions with: all categories of personal data, including usage data if applicable, HR2day and subprocessors process on behalf of institutions; legitimate business objectives HR2day and subprocessors are allowed to process personal data for and under which conditions; purposes HR2day and subprocessors are not allowed to process personal data for; audit right	The deadline for this is 31-12-2026.

		and subprocessors are not allowed to process personal data for; audit right for institutions with regard to the DPA.	for institutions with regard to the DPA.	
			Update privacy statement HR2day.	HR2day will update their privacy statement by 1-8-2026.
16.7	Loss of control of user satisfaction data		Include this processing within the scope of the DPA with HR2day as the processor and give institutions meaningful control (through transparency) and choices in this processing.	HR2day will include this in the DPA by 31-12-2026 and give institutions the option to turn this functionality off.
16.8	Loss of control and loss of confidentiality by unauthorised access in third countries	Stop using SignRequest	Identify all transfers, at least to Expo and Google	The deadline for this is 31-12-2026.
			Include lawful transfers to subprocessors in DPA between HR2day and institution.	The deadline for this is 31-12-2026.
			Inform institutions about parties personal data is being transferred to and they need to	The deadline for this is 31-12-2026.

			conclude agreements with directly.	
			Enable customers who stop using SignRequest to obtain a copy of their data subjects' processed data and delete them when necessary.	SignRequest already removes a customer's environment, including the personal data, one month after the customer stops using their services. HR2day will verify by 31-12-2026 that this deletion includes all personal data from institutions' data subjects and that institutions can obtain a copy of the personal data.
16.9	Loss of control of subprocessors and recipients through lack of or incorrect agreements		Perform assessment if Google and Apple qualify as subprocessors, joint controllers or third party recipients.	The deadline for this is 31-12-2026.
			Include Google and Apple in DPA between HR2day and institutions.	The deadline for this is 31-12-2026.
			Conclude the necessary agreements with Google and Apple.	The deadline for this is 31-12-2026. HR2day strives to have concluded subprocessor agreements with all subprocessors by 1-8-2026.
16.10	Loss of confidentiality due to absence	Implement 'read access logging' on categories of sensitive and	Enable 'read access logging' on categories of sensitive and special data and for	HR2day will have read access logging available for institutions on 31-

	of 'read access logging'	special data at the minimum.	the proxy login functionality at the minimum.	12-2026. Additionally, HR2day will start a working group with institutions.
		Implement read access logging for activities administrators carry out using the proxy login.		
		Inform users without undue delay that they have been impersonated.		
16.11	Breach of data minimisation by including too broad lists for reasons for absenteeism	Only use a pick lists to collect information about the reason for employees' absence and a fixed set of fields to collect further information about their absence.	Provide instructions to institutions about how to use pick lists to collect sensitive and special categories of data.	HR2day states that it has implemented this in its development cycle and has shown how it warns users to not to include any information about the nature and cause of the absence. The deadline for this measure is 31-12-2026.
		Have the absenteeism pick list and the fixed set of fields evaluated by the privacy department, to ensure they are in line with GDPR requirement and available guidelines.		
		Ensure users of HR2day are properly instructed and trained about which types of data can be processed about		

		employees' absence.		
16.12	Lack of accuracy through manual registration of personal data	Only use open text fields with a clear purpose.	Provide instructions to institutions about how to use open text fields in a way that respects data minimisation principles.	HR2day states that it has implemented this in its development cycle. HR2day warns to be careful using merge fields which contain sensitive data in the screen for alert setting. The deadline for this measure is 31-12-2026.
		Formulate questions in a way that makes it clear what (sensitive/special) personal data should and shouldn't be provided in an open text field and use the available information icons.	Provide sufficient options for field validation to prevent inaccurate data processing.	HR2day states that it has implemented this in its development cycle and shown field validation for bsn numbers and IBANs. The deadline for this measure is 31-12-2026.
		Ensure users of HR2day are properly instructed and trained about which types of data can be processed in open text fields.		
16.13	Lack of accuracy through manual registration of personal data	Automate input where possible, for example by connecting HR2day to the hiring system.	Provide sufficient options for field validation to prevent inaccurate data processing.	HR2day states that it has implemented this in its development cycle and shown field validation for bsn numbers and IBANs. The deadline for this
		Ensure HR employees are		

		properly instructed and trained in the institutions' procedures for carefully registering personal data.		measure is 31-12-2026.
16.14	Loss of control of retention periods because of lack of automation	Determine and manage retention periods for personal data in HR2day.	Provide information and instructions about the procedure to delete data using signal lists to institutions.	HR2day is in contact with two institutions and working on (i) desired level of granularity of retention periods (generic vs per data group) and (ii) the degree of uniformity between institutions. The deadline for these measures is 31-12-2026.
		Ensure the retention periods are complied with by establishing processes to enforce them, for example by using the automated retention periods for documents.	Facilitate institutions in enforcing their retention periods by improving the options for technical configuration and management of retention periods per group of personal data in HR2day.	
16.15	Loss of confidentiality due to vertical inheritance of rights default setting	Turn the vertical inheritance of rights off, unless it's necessary to use this setting.	Proactively inform institutions about the privacy implications of the vertical inheritance of rights setting and offer them the choice to turn it on or off.	The deadline for this is 31-12-2026.
		Restrict access to personal data for roles who don't need access to these data to perform their duties.	Cooperate with institutions to improve the options to respect the data minimisation principle while having the vertical inheritance of rights setting on, reducing the administrative burden OR enable them to carry out the	
		Be transparent to data subjects about the usage of the vertical		

		inheritance of rights setting and who has access to their data.	necessary workflows while having the setting turned off.	
16.16	Loss of confidentiality through lack of encryption key management	Assess if cell-level encryption, encryption with customer-managed keys and any other additional measures are necessary for special and sensitive categories of data, taking into account the specific data being processed by the institution and the other security measures in place.	Inform institutions about the encryption methods being used for the HR2day application and platform and about the possibility of additional safeguards, like cell-level encryption and encryption keys managed by HR2day.	HR2day will have additional safeguards available for institutions on 31-12-2026. The possibility for institutions to manage their own encryption keys already exists. Additionally, HR2day will start a working group with institutions to assess the desired options.
			Cooperate with institutions in assessing the necessary level of encryption for the personal data in HR2day, specifically for the sensitive and special categories of personal data.	
			Where institutions deem it necessary, implement additional safeguards, like cell-level encryption and encryption keys managed by HR2day.	
Mobile app risks				
16.17	Loss of control of personal data being processed due to installing of mobile app through third-party app store	Enable access through mobile browser from mobile devices.	Make the app available as side load.	HR2day will contact institutions about their wishes in this regard.
		Perform proportionality and subsidiarity assessments on	Enable access through mobile browser from mobile devices.	HR2day will contact institutions about their wishes in this regard.

		the provision of mobile app via app stores and ‘side-loading’ and implement the results.		
16.18	Loss of control due to processing of push notifications by Google and Apple	Don’t include personal data in the messages sent through push notifications.	Optional: Implement unified push for Android users.	HR2day will take no steps for this optional measure.
		Perform proportionality and subsidiarity assessments on sending push notifications via Google and Apple or Unified Push and implement the results.		

Introduction

HR2day is an application for human resource management (HRM) and payroll management, owned by the company of the same name. It's a software-as-a-service (SaaS) solution, deployed on the Salesforce platform-as-a-service (PaaS). HR2day is able to connect to other applications through an API. This DPIA will discuss the personal data processing that happens when HR2day is used.

SURF
SURF is the Dutch IT cooperative of education and research. It is owned by its members, comprised mostly of educational institutions and research institutions. Through SURF, they work together to, amongst other, procure the best possible digital services and develop and share knowledge with each other. Part of SURF's services is conducting DPIAs on IT services that a lot of members use.

DPIAs
DPIA stands for Data Protection Impact Assessment and this must be performed by data controllers when they process personal data in a way that may "result in a high risk to the rights and freedoms of natural persons", according to article 35 of the General Data Protection Regulation (GDPR). The assessment is intended to shed light on, among other things, the specific processing activities, the inherent risk to data subjects, and the safeguards applied to mitigate these risks. The purpose of a DPIA is to ensure that any risks attached to the process in question are mapped and assessed, and that adequate safeguards have been implemented to mitigate those risks.

Data subjects have a fundamental right to protection of their personal data and some other fundamental freedoms that can be affected by the processing of personal data, such as freedom of expression. The right to data protection is therefore broader than the right to privacy. Consideration 4 of the GDPR explains:

> *"This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity"*.

Reference DPIAs versus individual DPIAs
In GDPR terms, SURF is not the data controller for the processing of personal data via the use of HR2day. Each individual educational or research institution that uses HR2day is the data controller. However, as the Dutch IT cooperative, SURF takes the responsibility to assess the data protection risks for the end users and to ensure the data processing complies with the GDPR. Therefore, SURF conducts reference DPIAs to assist its members to select a privacy-compliant deployment, and conduct their own DPIAs where necessary. Only the organisations themselves can assess the specific data protection risks, related to the technical privacy settings, nature and volume of the personal data they process and vulnerability of the data subjects. The Dutch DPA has endorsed this approach to improve

the protection of personal data within the Education sector.[1] This reference DPIA is meant to help educational and research organisations with the DPIA they must conduct when they deploy HR2day, but it cannot replace the specific risk assessments the organisations must make themselves.

Performing one reference DPIA on an IT service has benefits for SURF's members, as well as for the vendors of the products SURF assesses. For the members, it saves the cost of each of them having to do an entire DPIA individually. They are also able to incorporate their combined knowledge about a product and experiences with a vendor in the reference DPIA. Additionally, SURF can more effectively negotiate mitigating measures with the vendors, because it has the combined negotiating power of the entire sector as a representative. For the vendors, it saves time, effort and money as well to not have to assist every institution individually with DPIAs that will likely be very similar. It's also more efficient for them to be able to implement measures that benefit all members at once.

DPIA criteria
The Dutch Data Protection Authority (Dutch DPA) has published a list of seventeen types of processing for which a DPIA is always mandatory in the Netherlands. If a processing is not included in this list, an organisation must itself assess whether the data processing is likely to present a high risk. The European national supervisory authorities (hereinafter referred to as the Data Protection Authorities or DPAs), united in the European Data Protection Board (EDPB) have also published a list of nine criteria. As a rule of thumb if a data processing meets two of these criteria a DPIA is required.

From the EDPB list, number 4, 5 and 7 apply, as they probably will for most HR systems.

- *Number 4 – Sensitive data or data of a highly personal nature*: Due to the nature of HR2day as a HR system, it contains special categories of data and sensitive data.
- *Number 5 – Data processed on a large scale*: The personal data in HR2day concerns all employees and non-salaried personnel of an institutions and these people may be working there for a long time, causing their data to be processed for a long time as well.
- *Number 7 – Data concerning vulnerable data subjects*: There is a power imbalance between employers and employees.

Scope
HR2day is divided in modules. Every module contains a certain set of functionalities. This DPIA has examined the following modules:

[1] Dutch DPA (in Dutch only), Sectorbeeld Onderwijs 2021-2023, 24 January 2024, p. 5-6, URL: https://www.autoriteitpersoonsgegevens.nl/documenten/sectorbeeld-onderwijs-2021-2023.

Module	Features
Personnel and payroll administration	Automated and accurate payroll administration and a complete digital employee file and contract management.
Self-service (ESS/MSS)	ESS: Employee Interaction Centre, where employees can manage their own affairs. MSS: Manager Interaction Centre, where managers can manage their team members' affairs.
Leave	Submission of requests for and management of leave in alignment with company policy and collective labour agreements.
Absences	Management of absences because of sickness and other reasons, as well as support for communication with external parties such as the UWV.
Expense claims	Submission and management of expense claims.
Document management	A digital file with all documents related to employees in the organisation.
Reports	Generating and exporting reports based on the data in HR2day.
Digital signature	Signing (legal) documents digitally.
HR analytics	Provides (real time) insights and analyses for HR data.
Employee feedback	Management and monitoring of the performance and development of employees.
"Arbokoppeling" (API)	Enables data to be exchanged between HR2day and occupational health and safety service systems.

The Salesforce platform which HR2day is built on is also within scope, since it is such an integral part of the application.

Out of scope

- The following modules were placed out of scope due to the lack of use by institutions:
    - Education management
    - 360 Degrees feedback
    - Surveys
    - Portfolio
    - Formation and budget
    - Sandbox

- Since most people in the working population are adults, this DPIA assumes the processing of personal data of minors as users in HR2day is an exception. This scenario is not in scope of this DPIA.

Methodology
This DPIA was created through a combination of documentation review, technical research and explanations provided by HR2day in response to questions.

The documentation review consists of requesting and analysing agreements, policy documents, procedures and information security certifications. HR2day was also given the opportunity to respond to findings, as specific follow-up questions were asked. This part of the investigation focused primarily on the legal agreements that have been established with regard to the processing of data in HR2day.

The technical investigation within the DPIA analyses the technical aspects of HR2day using use case scenarios.[2] This investigation ties in with the legal findings and examines how data is collected, processed, stored, shared and secured. Technical analysis of data flows, storage methods, logging, security measures and privacy settings is used to assess whether the technical implementation complies with GDPR requirements:

1. Intercepting network traffic while executing test scenarios in the application.
2. Analysing technical documentation.
3. Analysing the data resulting from data subject access requests.

The technical documentation is also examined, and questions have also been posed to HR2day in this regard.

Outline
This DPIA is based on the Dutch model DPIA for government agencies.[3] This model is well suited to the activities carried out by educational and research institutions, as they also perform duties in the public interest. Since this is a referenceDPIA, changes have been made to the structure of the original model where necessary.

The model consists of four parts.

A. Part A describes the facts of the data processing operations;
B. Part B assesses the lawfulness of the facts processed in Part A;
C. Part C deals with the risks to the rights and freedoms of data subjects; and
D. Part D deals with the measures envisaged to address those risks.

Timeline
This DPIA was started in January 2025 and finished in May 2026.

[2] Appendix 1.1

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

Part A. Description of the processing

1 HR2day

HR2day is an all-round HRM system that supports a number of processes with a fixed data model. This means the structure, fields and categories of data that customers can enter are entirely determined by HR2day. HR2day provides default processes that can be tailored for the use of the individual institution.

This chapter serves as an introduction to the system. It will give a general overview of the functionalities, architecture and components of the system, the applicable security certifications and the company that owns it.

1.1 HR2day – HR and payroll in one application

HR2day supports the entire employee journey from onboarding to offboarding and everything in between.

HR2day is built to be flexible and modular, customers can specify the system (workflows) to their needs and can choose from a wide array of modules to support their needs.

Talent Management	Self Service	HR & Payroll	HR Analytics
Recruitment	Employee self service	Staffing and budgeting	Business reporting
Performance management	Manager self service	Personnel administration	Business control
Training management	Workflows	Digital dossier	Business intelligence
Competency management		Organisation management Payroll processing	
Portfolio management		Leave Absence	
		Expense claiming	

Tabel 1-1, HR2day modules[4].

HR2day is configured based on collective labor agreement (CAO) conditions, enabling it to create clusters of employment terms to ensure compliance with said CAO. The system also links employee data to their employment relationship, making this relationship the fundamental basis for the employee's record within the system.

[4] From presentation HR2day.

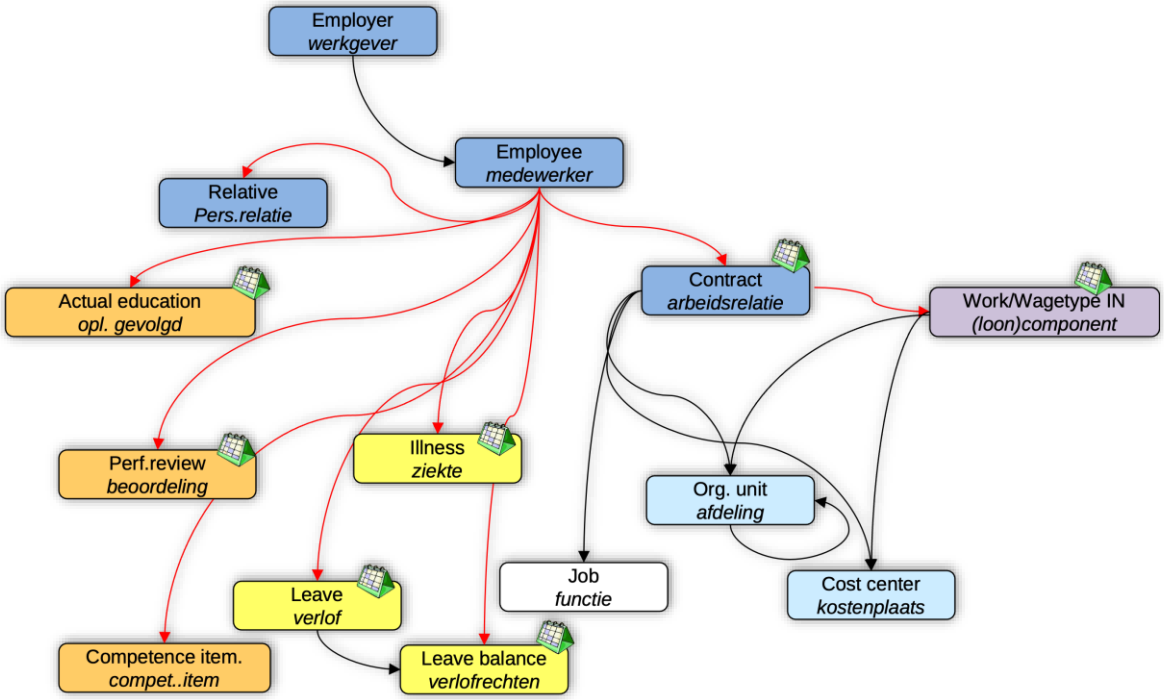

Figure 1-1, HR-data vs. payroll data from presentation HR2day.

1.2 Salesforce architecture

HR2day is a cloud-based SaaS application built to run natively on the Salesforce platform, using core Salesforce technologies/services to deliver a scalable HR experience. Its deep integration with Salesforce is central to its design. Because of the importance of the Salesforce platform for HR2day, this DPIA will also focus on data processing through Salesforce.

> *"Native Force.com applications are built entirely on the Force.com platform. These native apps sit inside the Salesforce infrastructure and are hosted, managed, and delivered by salesforce.com."*[5]

HR2day emphasizes it chose Salesforce's platform because of the security certifications Salesforce offers. For more information, see 1.3 Security.

1.2.1 Salesforce platform components used by HR2day

- **Lightning** provides a consistent user experience across desktop and mobile devices, benefiting from Salesforce's ongoing development of this service. It is a component-based framework for app development on Salesforce platform.
- **Hyperforce** is Salesforce's next-generation infrastructure foundation for deploying application stacks on commercial cloud providers and enables customers to choose regions where their data is hosted.

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

- **Login** provides authentication and user management through Salesforce's login and identity services. HR2day inherits Salesforce's security, including single sign-on (SSO), multi-factor authentication (MFA), and user provisioning[6].
- **Visualforce** provides a custom UI. This allows for tailored workflows or forms that go beyond standard Lightning components.
- **Content** provides file management to management documents, policies, and employee files. This includes secure, centralized, and document storage with access controls.
- **Experience Cloud Sites** extends disclosing beyond internal users. In the case of HR2Day it provides the login page.
- **Heroku** for building and running custom applications (i.e. PDF generator) or microservices that need to interact with Salesforce data but require technologies or frameworks not natively supported by Salesforce.

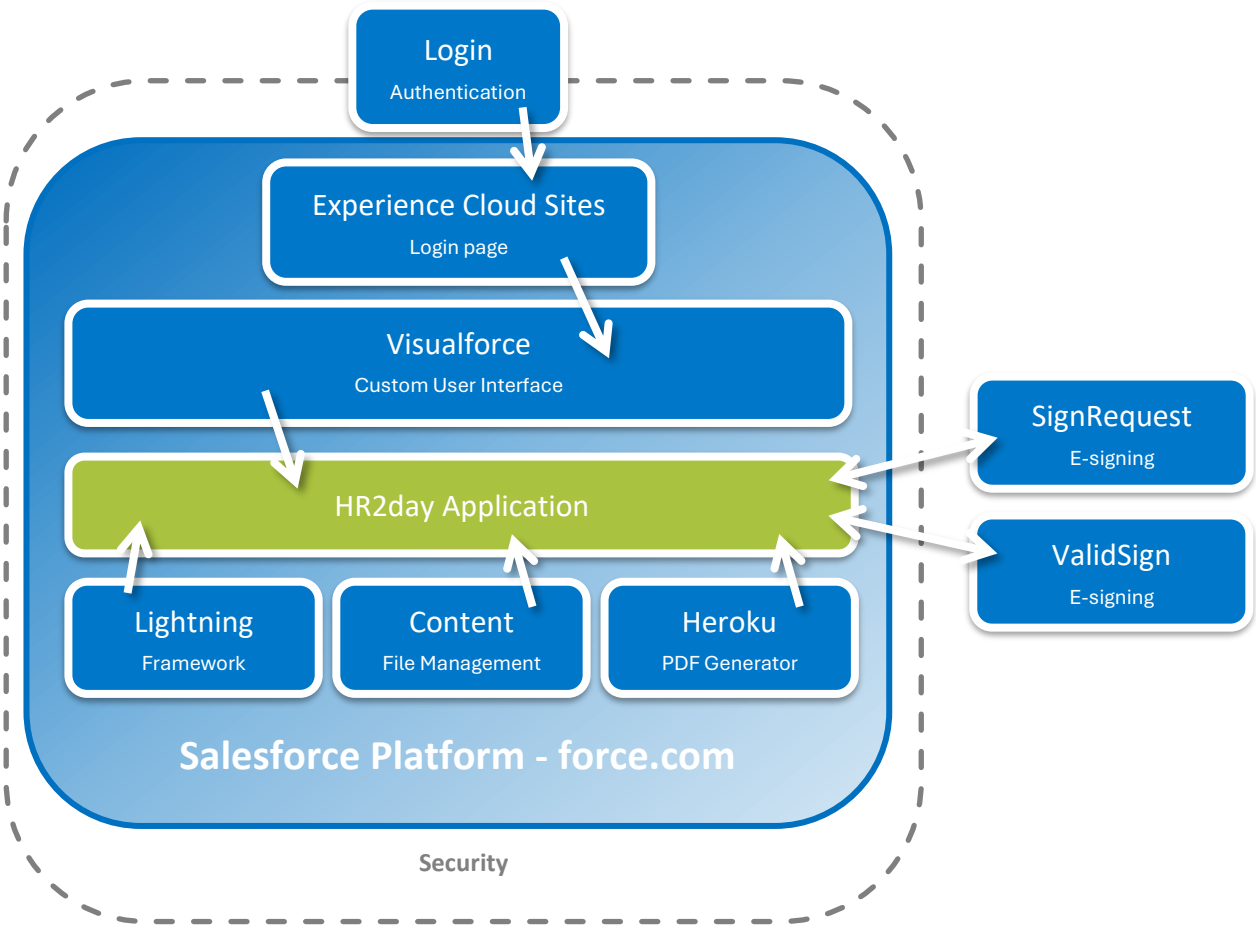

Figure 1-1 Schematic representation of architecture.

1.2.2 Salesforce's security framework

HR2day uses Salesforce's security infrastructure, including authentication, access controls, and encryption. This means the privacy and security of HR2day are closely tied to Salesforce's own compliance certifications and practices. Salesforce follows the Shared

[6] Creating, managing, updating, and removing user accounts and their access rights.

Responsibility Model, according to which HR2day is responsible for securing the HR2day application, which is built on the Salesforce platform.[7]

1.2.3 Salesforce's compliance framework

Salesforce provides HR2day resources and documentation specifically to support DPIAs, helping organizations assess how Salesforce's technical and organizational measures align with GDPR and other data protection regulations.

HR2day can make use of Salesforce's tools[8] for data subject access requests, data export, and deletion.

1.3 Security

HR2day has an ISAE 3402 type II report with a carve-out for Salesforce's services. Salesforce has an ISO 27001 certification and a SOC 2 report for their services on Hyperforce, which HR2day relies on and checks periodically. Arranging these security certifications this way is an industry standard for SaaS-providers on platform services.

1.4 HR2day+ App

HR2day uses Salesforce as its platform and publishes its mobile application named HR2day+ on Google Play Store and Apple App Store respectively. The app is a hybrid app that uses a web view to display the HR2day web application from the Salesforce platform in a mobile environment. This means the app is a native shell that loads and displays the Salesforce-hosted web application within a mobile environment.

The mobile application uses the same sub processors as its web-based counterpart and uses one extra sub-processor for sending notifications (see 4.4.3 Receiving notifications).

1.5 HR2day B.V.

HR2day B.V. is the company that exploits the application HR2day. The company is owned for 70% by Visma Nederland B.V., which is part of the European Visma Group. The Visma Group is the parent company of more than 200 subsidiaries like HR2day B.V. It has an overarching strategic role and general frameworks and guidelines have been drawn up for the subsidiaries. It has a layered hierarchical organisational structure in which the subsidiaries have operational autonomy, including some freedom in legal matters. However, in the area of privacy, autonomy is more limited and subsidiaries must comply with the central guidelines and frameworks established by the Visma Group. For example, the Visma Group has a comprehensive Data Protection Programme that includes policy, guidelines, risk and maturity monitoring, incident handling, awareness, and mandatory privacy training for all employees.[9]

To ensure that the careful handling of personal data is embedded in the daily activities and services of all subsidiaries, each subsidiary has a Data Protection Manager (DPM) who is

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

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

[9] Data Protection Program, https://www.visma.com/trust-centre/privacy/data-protection-program, accessed on 13 October 2025.

responsible for privacy within the company and reports to the Managing Director of the subsidiary. The Visma Group Legal & Compliance Team assists and advises the DPMs in their daily data protection activities and reports regularly to the Board of Directors via the Risk Audit Committee. The Visma Compliance Council is the advisory body for Visma Group and its companies with regard to compliance with EU laws and regulations. The GDPR receives extra attention due to the nature of Visma Group as a software supplier that processes a large volume of personal data and has more than 15,000 employees.

2 Purposes

This chapter is about the purposes that HR2day processes users' personal data for. Listing these purposes will give a general idea of what the product is used for.

A sample of processor agreements from HR2day's customers shows that purposes determined by HR2day's customers are personnel administration, further defined as "quick and efficient access to both individual and collective personnel information [...] in the interests of a responsible personnel policy for both individuals and the organisation as a whole" and complying with legal requirements.[10] There is no documentation explicitly stating that HR2day determines any of its own purposes for the data processing in HR2day as a processor.

In addition to these purposes found in the processor agreements, the purposes described below are based on the contracts and tender documentation between HR2day and their customers, descriptions of the different HR2day modules and the research into the actual processing operations. They are divided into purposes based on the functions described in the 'Hoger Onderwijs Referentie Architectuur' model (HORA) and other purposes. The HORA is a business function model for educational institutions. It describes the functions of an organisation, independently of how these functions are implemented in a specific organisation.[11] Since the HORA describes the essential functions of educational organisations on a high level, it is a good model to derive the main purposes for data processing in applications like HR2day from. Using the HORA as a reference also ensures that it will be easy for institutions to find the right place in their organisational structure to implement any measures or changes from this DPIA. The other category consists of 'supporting' purposes, which support the main processes.

2.1 HORA purposes determined by the institutions

The purposes below can be summarised as personnel and payroll administration.

2.1.1 Business operations - HRM

HR2day is, as the name suggests, a tool to support human resource and payroll processes. Therefore, the main purposes of the processing activities in this tool are connected to HRM.

1. **Formation planning**
   Deciding what budgets and positions there are available for the departments.
2. **Employee evaluation**
   Evaluating employee performance and deciding on remuneration and promotion as well as dismissal and demotion.
3. **Employee administration**
   Administering all employee data.
4. **Salary and expense processing**
   Calculating and paying employees' salaries and expense claims.
5. **Sickness and leave administration**

[10] Data Processing Agreement with [confidential]; Data Processing Agreement with [confidential]; Data Processing Agreement with [confidential]. SURF members can ask for access to these documents.

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

Recording employees' sickness and leave.

2.1.2 Direction - accountability

The information from HR2day is also used to gain insight into the organisation's functioning.

6. Internal reports

Making information about the organisation's functioning available to internal parties.

2.2 Supporting purposes determined by the institutions

Institutions use HR2day for the purposes described in paragraph 2.1. To ensure that HR2day functions effectively, efficiently and safely, HR2day processes personal data for the following purposes. Processing activities for these purposes are common for IT services, but they have not been defined in any HR2day documentation.

7. Providing the service and keeping it up-to-date

Carrying out the operations needed to ensure the service functions continually and as intended, like storage, hosting, fixing bugs, etc.

8. Securing the service

Ensuring the confidentiality, integrity and availability of data in the service and ensuring resilience of the service, amongst others through facilitating identification and authentication and making back-ups.

9. Personalising the service

Support individual user preferences and efficient information provision.

10. Providing customer support

Providing methods through which customers and users can request and receive support when encountering problems.

11. Improving the service

Making changes to the service in accordance with customers' wishes.

2.3 Purposes determined by HR2day

HR2day shared their privacy statement with SURF for this DPIA. It does not state explicitly if this statement applies to personal data collected through the HR2day application or not, but it does state that HR2day can collect data from data subjects who work for HR2day's customers. This group includes users of the application. HR2day commented that this statement does not apply to the HR2day application, except for the reference to the creation of accounts.[12]

In their privacy statement, HR2day determines some purposes for which they process personal data.

"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

[12] Comment on chapter 2.3 from review, 21 November 2025.

- 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]

[13] HR2day Privacy Statement, shared with SURF on 20 March 2025.

3 Personal data

According to article 4(1)(a) of the GDPR,

> *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

3.1 Categories of data subjects

As an HR-system, HR2day processes the following categories of data subjects:

- **Employees**[14]
- **Non-salaried staff**
- **Former employees and non-salaried staff**
- **Administrators**
- **Teacher**
- **Partners / Kids of (ex) employees**

Since most people in the working population are adults, this DPIA assumes the processing of personal data of minors as users in HR2day is an exception. This scenario is not in scope of this DPIA. Another way minors' data may be processed is when the names of employees' children are registered.

3.2 Processed personal data

3.2.1 Data Subject Access Request

As part of the technical investigation, Data Subject Access Requests (DSARs) were submitted to the vendor. These requests covered three data subjects – specifically, two employees and one HR manager – whose profiles were used to execute various scenarios within the system.

3.2.1.1 Data provided by the vendor

The vendor supplied the following data in response to the DSARs:

- Overview of employment relationships
- Record of changes to employment relationships
- Log of login activities
- Employee personal data
- Change logs of employee personal data
- Educational records
- Salary specifications
- Salary components

[14] For brevity, the term "employees" includes non-salaried staff and former employees and non-salaried staff when used in the running text. When used as a label, "employees" only refers to workers employed by an employer.

- Legal basis for each data category
- List of third parties with whom data is shared
- Data retention periods per personal data category
- Instructions for data subjects on how to access/update their own information (including clarification that certain data cannot be changed due to legal obligations)

3.2.1.2 Key findings from DSAR data analysis

Upon analysing the data provided, the following observations were made:

- Data submitted/processed by SignRequest (see 4.3.6.1) is absent.
- Security-related log data is missing.
- Log data intended for product improvement is absent.
- The categories of personal data do not align with those defined in sample of data processing agreements.[15]

3.2.2 Categories of personal data

For this DPIA, the personal data in HR2day have been divided into categories. Each category contains personal data items that have a similar nature. For a description of the categories, see Bijlage 2. Some personal data may fit into multiple categories. In that case, they get categorised in the category with the highest sensitivity.

In the tables below, some data items of a similar type have been grouped together in subgroups for brevity. For example, the subgroup 'Name' contains the name used to address someone, first name, last name, initials, nickname and prefixes. Likewise, the category 'Salary data' contains different types of data with different sensitivity levels. For the full overview of personal data items, SURF Vendor Compliance can be contacted.

Paragraphs 3.2.3 and 3.2.4 contain explanations on they categorisations of special categories of personal data and sensitive personal data.

The tables below contain all data fields that HR2day provides. Institutions can determine which fields are visible to users in the modules for personnel and payroll administration and absences.

Directly identifiable personal data

Personal data	Data subject	Sensitivity	Source
Name	Employees, Teacher, Partner / kid of (ex) employee, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system
Date of birth	Employees, Teacher, Partner / kid of (ex) employee, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system

[15] SURF performed its technical tests in its own environment, so the DPAs from the institutions do not apply to these tests. However, HR2day used its standard DSAR response with its standard data categories, which the institutions would also receive if they forwarded a DSAR.

Place of birth	Employees, Ex-employees, Teacher, Non-salaried staff	Special (in combination with nationality)	Data subject or other users of the system
ID data	Employees, Ex-employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Bank account data	Employees, Ex-employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
User	Employees, Ex-employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Signature	Employees, Ex-employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
ID number	Employees, Ex-employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Employee number	Employees, Ex-employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
IBAN	Employees, Ex-employees, Teacher	Normal	Data subject or other users of the system
Photo	Employees, Ex-employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
National identification numbers	Employees, Ex-employees, Teacher, Non-salaried staff	Sensitive	Data subject or other users of the system

Contact data

Personal data	Data subject	Sensitivity	Source
Address	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Email address	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Phone number	Employees, Teacher, Partner / kid of (ex) employee, Non-salaried staff	Normal	Data subject or other users of the system
Postal code	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system

Demographic data

Personal data	Data subject	Sensitivity	Source
Title	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Gender	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Age	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
State pension date	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Nationality	Employees, Teacher, Non-salaried staff	Special (in combination with country/place of birth)	Data subject or other users of the system
Country of birth	Employees, Teacher, Non-salaried staff	Special (in combination with nationality)	Data subject or other users of the system
Civil status	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Education	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Employment history	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Relationship type	Employees, Teacher, Partner / kid of (ex) employee, Non-salaried staff	Normal	Data subject or other users of the system

Organisational data

Personal data	Data subject	Sensitivity	Source
Contractual data	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Department	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Place of work	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Position	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system

Part-time factor	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Ancillary activities	Employees, Teacher, Non-salaried staff	Normal, possibly sensitive or special	Data subject or other users of the system
Owner account	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Reviews	Employees, Teacher, Non-salaried staff	Normal, possibly sensitive or special	Data subject or other users of the system
Agreements education	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Competences	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Absence data	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Leave data	Employees, Teacher, Non-salaried staff	Normal	Data subject or other users of the system
Payments	Employees, Teacher, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system
Contractual data	Employees, Teacher, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system
Documents	Employees, Teacher, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system
Notes	Employees, Teacher, Non-salaried staff, Ex-employees	Normal, possibly sensitive or special	Data subject or other users of the system
Employment relationship	Employees, Teacher, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system
Activities	Employees, Teacher, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system
Events	Employees, Teacher, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system

Conversation records	Employees, Teacher, Non-salaried staff, Ex-employees	Normal, possibly sensitive or special	Data subject or other users of the system
Emails	Employees, Teacher, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system
Salary data	Employees, Teacher, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system
Insurance data	Employees, Teacher, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system
Wage garnishment	Employees, Teacher, Non-salaried staff, Ex-employees	Normal	Data subject or other users of the system

Health data

Personal data	Data subject	Sensitivity	Source
Absence data	Employees, Ex-employees, Teacher, Non-salaried staff	Special	Data subject or other users of the system
Tax data	Employees, Ex-employees, Teacher, Non-salaried staff	Special	Data subject or other users of the system
Salary data	Employees, Ex-employees, Teacher, Non-salaried staff	Special	Data subject or other users of the system
Pension data	Employees, Ex-employees, Teacher, Non-salaried staff	Special	Data subject or other users of the system
Benefits	Employees, Ex-employees, Teacher, Non-salaried staff	Special	Data subject or other users of the system
Employment relationship	Employees, Ex-employees, Teacher, Non-salaried staff	Special	Data subject or other users of the system

Financial data

Personal data	Data subject	Sensitivity	Source
Salary data	Employees, Ex-employees,	Sensitive	Data subject or other users of the system

	Teacher, Non-salaried staff		
Expense claims	Employees, Ex-employees, Teacher, Non-salaried staff	Sensitive	Data subject or other users of the system
Documents	Employees, Ex-employees, Teacher, Non-salaried staff	Sensitive	Data subject or other users of the system
Contractual data	Employees, Ex-employees, Teacher, Non-salaried staff	Sensitive	Data subject or other users of the system
Travel data	Employees, Ex-employees, Teacher, Non-salaried staff	Sensitive	Data subject or other users of the system
Wage garnishment	Employees, Ex-employees, Teacher, Non-salaried staff	Sensitive	Data subject or other users of the system
Employment relationship	Employees, Ex-employees, Teacher, Non-salaried staff	Sensitive	Data subject or other users of the system
Benefits	Employees, Ex-employees, Teacher, Non-salaried staff	Sensitive	Data subject or other users of the system
Pension data	Employees, Ex-employees, Teacher, Non-salaried staff	Sensitive	Data subject or other users of the system
Life annuity	Employees, Ex-employees, Teacher, Non-salaried staff	Sensitive	Data subject or other users of the system

Trade union data

Personal data	Data subject	Sensitivity	Source
Salary data (offset for trade union membership fees)	Employees, Ex-employees, Teacher, Non-salaried staff	Special	Data subject or other users of the system

Political data

Personal data	Data subject	Sensitivity	Source
Salary data (political leave)	Employees, Ex-employees, Teacher, Non-salaried staff	Special	Data subject or other users of the system

Technical/diagnostic/logging data

Since this is an reference DPIA, which primarily focuses on risks that are inherent in using the service the vendor provides, the technical/diagnostic/logging data that vendors usually collect are of special interest. The processing of these data can happen in the background without users and admins having a way to know about it, which can cause a lack of transparency. The table below shows the technical/diagnostic data the research for this DPIA showed. However, since the response to the DSARs was missing information, this datasets completeness has not been verified.

Personal data	Data subject	Sensitivity	Source
Logging[16]	Employees, Ex-employees, Teacher, Non-salaried staff, Administrators	Normal	System
Cookie collected data[17]	Employees, Ex-employees, Teacher, Non-salaried staff, Administrators	Normal	Data subject, system
Device data	Employees, Ex-employees, Teacher, Non-salaried staff, Administrators	Normal	System

3.2.3 Special categories of personal data

Article 9 of the GDPR prohibits processing of special categories of personal data, which consist of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. These types of personal data can only be processed when an exception from article 9 paragraph 2 applies. Most of the special categories of personal data of data in HR2day are health data.

Institutions can register in HR2day when employees are absent, for example due to illness or pregnancy and classify the data about the illness. They are able to determine their own categories for this. HR2day does not offer fields to register the cause of the illness.[18]

Employees' illness also influences their sick pay, and therefore their salary. Furthermore, HR2day contains data about users who qualify for certain benefits, tax benefits or work provisions due to illness or being disabled. Therefore, some types of tax data, salary data, pension data and data about the employment relationship qualify as health data.

[16] For full list of logged data see annex 1.5.

[17] For full list of cookies see annex 1.4.

[18] Look at Beleidsregels verwerking persoonsgegevens gezondheid zieke werknemers (https://wetten.overheid.nl/BWBR0037896/2016-04-29, accessed on 23 Januari 2026) to see what data employers are allowed to register about sick employees.

HR2day can contain political and trade union data as well. Employers can grant political leave and offset trade union membership fees for employees, affecting their salary.

Furthermore, the nationality in combination with the place, country of birth and photo shows a data subject's racial or ethnic origin and is therefore a special category of personal data.[19]

Lastly, reviews, notes, conversation records and ancillary activities can contain special categories of personal data, depending on what is registered by the institution. For example, these fields could contain notes on employees' activities for a political party, notes on how someone's health condition is affecting their performance, notes on what their needs to practise their faith at work are or notes on employees feeling discriminated at work due to their sexual orientation. Due to the nature of these fields, there is a real possibility these types of data are processed.

3.2.4 Sensitive personal data

Some personal data aren't special according to article 9, but can be sensitive because of their relatively big impact on someone's privacy.[20] All personal data revealing information about someone's financial situation qualify as sensitive.

There is a lot of financial data in HR2day, mostly about employees' salary. HR2day can also be used to register how the employment relationship between employees and their employers impacts their salary, how employees' pensions are impacted by certain circumstances, whether there is wage garnishment on someone's salary and if someone gets any benefits.

Reviews, notes, conversation records and ancillary activities can also contain sensitive data due to the nature of these fields. They can contain information that employees share with their managers, but which they wouldn't feel comfortable sharing with other people. Examples are information about their home situation, family members' health and financial issues.

Lastly, users can upload any document without restriction and due to the nature of HR2day as an HRM system, there is a possibility documents contain sensitive data. One example is declarations, which contain information about employees' financial situation.

3.2.5 National identification number

Employers can register national identification numbers in HR2day. They are required to register these for tax purposes and are only allowed to process them in accordance with the Wages and Salaries Tax Act.[21]

---

[19] Autoriteit Persoonsgegevens, Personeelsdossier, https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/personeelsgegevens/personeelsdossier, accessed on 16 October 2025.

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

[21] BSN at work, https://www.autoriteitpersoonsgegevens.nl/en/themes/identification/citizen-service-number-bsn/bsn-at-work, accessed on 13 October 2025.

3.3 Sources of personal data

According to article 13 and 14 of the GDPR, data subjects must be informed about data processing with their personal data, whether they have been collected directly from them or not. The personal data in HR2day can come from several sources. It's possible to connect HR2day to a recruitment system, so (part of) the data can automatically be imported from that system. Users can also enter personal data about (new) employees manually, either about themselves or other employees. Therefore, the personal data in HR2day is imported from a recruitment system, collected directly from the users, entered by other users of the system or generated based on data that is already present in the system or users' behaviour.

4 Processing activities

This chapter will describe the processing activities that can take place in HR2day. According to article 4 paragraph 2 GDPR, processing is defined as follows:

> *"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;"*

The processing activities as described in the processor agreements are "the processing of personal data in the context of payroll and personnel administration". The descriptions below go into more detail and are based on the actual processing operations as found in the research for this DPIA.

The building blocks of HR2day are processes. In HR2day, these processes take the form of workflows. Theys are defined by the types of activities and actions institutions can perform on data, like submitting and approving/denying. This part of the processing operation can be described as the 'how'. Within HR2day's data model, institutions are free to decide the types of data they want to use in these processes. This part of the processing operation can be described as the 'what'. So, the processing operations for different institutions may look different based on the way they have implemented the processes HR2day offers, although some processes are less flexible than other. This chapter will describe the 'how', so the different processes HR2day offers. It will also describe the personal data that gets processed in some processes in the default configuration (the 'what'). However, it is important to bear in mind that the personal data, as described in chapter 3, that institutions process using the HR2day's process may differ from the default.

This chapter uses labels to show the relationships between the processes and the other components of this DPIA, like the types of personal data and the purposes.

4.1 Collection

4.1.1 On boarding

Purposes	Employee administration	Authentication	Salary and expense processing	
Data Sensitivity	Directly identifiable	Financial	Organisational	Etc.
	Normal		Sensitive	
Data subjects	Employees		Non-salaried staff	

On boarding, or creating new employees in HR2day, can take place through a workflow (see paragraph 4.3.2), but it's also possible to do it 'manually'. This workflow is included in the default set-up of HR2day. To create a new employee in HR2day, a manager first creates a new "arbeidsrelatie" to fill out all the personal data about the new employee, their role in

the organisation and their terms of employment. All data about the new employee under the "arbeidsrelatie" then automatically gets copied to their record under "HR gegevens". The information about the "arbeidsrelatie" also becomes part of the "HR gegevens".

After that, a user account gets created for the employee to be able to use HR2day and a profile gets assigned to the user. This happens semi-automatically. All data get defaulted from the employee data and then the admin has to select the right profile. The rights a user gets in HR2day are based on the profile. (See chapter *4.3.9 Managing roles and profiles* for more information about the rights structure) It's also possible to assign additional roles to employees, which determine which other employees are visible to the user. For example, managers of a department can view all employee data from the employees in that department.

4.2 Storing data

Purposes	Employee administration	Authentication	Salary and expense processing	
Data	Directly identifiable	Financial	Organisational	Etc.[22]
Sensitivity	Normal		Sensitive	
Data subjects	Employees		Non-salaried staff	

Almost all data in HR2day gets stored in data centres in France and Germany. More information about this in chapter 9.

Data processed by sub-processor SignRequest is processed in the US.

See ***Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.***.

4.3 Use

4.3.1 Signing in/off

Purposes	Securing the service		
Data	Directly identifiable	Organisational data	Technical/diagnostic data
Sensitivity	Normal		
Data subjects	Employees	Non-salaried staff	Administrator

Users can sign in with their user account or through single sign-on. The service implements Single Sign-On (SSO) functionality to streamline and secure user authentication. Users may access the service either through the native Salesforce login page, which includes Multi-Factor Authentication (MFA), or by using their institution's own SSO solution. The SSO service is provided by a party that implements SSO on Salesforce. Institutions make

[22] Instead of listing all categories, the table uses " Etc." to indicate all types of data are involved.

agreements directly with this party. HR2day uses cookies to ensure the user stays logged in during the session.

These cookies are used for authentication:

Cookie name	Age	Description
RSID		Session ID and login as session ID. Cookies copied to response and cause target URL to rebuild appropriately in a proxy situation.
SUCSP	Session	Used when the user identity that an admin is assuming, via Log In as Another User, is a Customer Success Portal (CSP) user.
SUPRM	Session	Used when the user identity that an admin is assuming, via Log In as Another User, is a Partner Relationship Management (PRM) portal user.
sid	Session	Session ID used to authenticate Lightning Platform Soap-API and Rest-API data connections for the current user.
sid_Client	Session	Used to detect and prevent session tampering.
autocomplete	60 Days	Determines if the login page remembers the user's username.
disco	Session	Tracks last user login and active session for bypassing login (e.g., OAuth immediate flow).
lloopch_loid	1 Year	Determines whether to send the user to a specific portal login or an app login.
login	60 Days	If the user's session has expired, used to fetch the username and populate it on the main login page when using process builder app.

Tabel 4-1, cookies used in signing in/signing off.

4.3.2 Workflows

Purposes	Employee evaluation	Employee administration	Salary and expense processing	Sickness and leave administration
Data	Directly identifiable	Contact information	Organisational data	
	Demographic data	Communication data	Health data	
Sensitivity	Normal	Sensitive	Special	
Data subjects	Employees	Non-salaried staff	Ex-employees	Partner / kid of (ex) employee

Institutions can design their own workflows in HR2day. Workflows are processes that consist of a series of steps that automatically follow each other up. They exist to make standard tasks, that follow same steps every time, easier. Examples are filing requests for

leave, filing absence due to illness, filing expense claims and submitting changes to HR records, like address, bank account number, civil status and competences.

These steps consist of employees/managers submitting changes and can also include an approval or a rejection by another person. Each rejection is accompanied by an explanation in an open text field. Entering information in workflows is possible through dropdown menus, multiple choice check boxes, free text fields that can be long or short and through adding documents. Different roles can have access to different workflows, or different steps in different workflows. The creation of and changes to certain data in the workflow are also logged (see *4.3.10 Logging)*. Employees and manager get access to different workflows. For example, employees can submit leave requests, call in sick and submit changes in their contact data, while managers can make changes to the contracts and salary of their employees.

Employees get an overview of the ongoing processes that they initiated themselves. On top of that, they get notifications for actions they need to take. These signals can lead to employees having to initiate a workflow. Employees don't get an overview of the workflows that involve them which their managers have started.

Institutions are free to design their own workflows, but in the standard configuration of HR2day, there are some workflows already present. It's also possible to delete these standard workflows.

4.3.3 Accessing personal data through the EIC and MIC

Purposes	Employee administration	Salary and expense processing	Sickness and leave administration
Data	Directly identifiable	Contact Information	Demographic Data
	Communication Data	Health Data	National Identification Number
	Behavioural Data	Racial and/or Ethnic Data	Financial Data
Sensitivity	Normal		Sensitive
Data subjects	Employees	Non-salaried staff	Ex-employees

In the Employee Interaction Centre, employees can access the following information:

- An overview of actions the employee can take, which will start workflows.
- An overview of their department calendar, which shows the absences of their team. The calendar doesn't show the difference between absences ('verzuim') and leaves by default, but it is possible for the employers to make this difference visible.
- Their salary specifications. Their salary is blurred by default and they must click it to see.
- An overview of notifications, which they can turn off.
- An overview of their leave.
- An overview of absences, other than leave.
- A graphic of their development.
- An overview of pending actions, ongoing processes and completed processes.

- The amount of open expense claims and expense claims that are being processed, with the option to show the declarations themselves.
- An overview of personal relationships.
- On overview of links.
- Access to their documents which can contain:
    - Copy of identification papers
    - Salary Specifications
    - C.V.
    - Contracts
    - And other documents that are filed in the employee dossier

The Manager Interaction Centre works in the same way, with two differences:

- Since managers have extra authorisations to access data from employees in their team, they can access that information in their MIC (see *4.3.9 Managing roles and profiles*).
- Managers have additional access to:
    - Birthdays.
    - Possible reports they can generate.
    - The types of absences in the calendar for members of their team.

4.3.4 Accessing and editing the employee record (directly)

Purposes	Employee administration	Salary and expense processing	Sickness and leave administration
Data	Directly identifiable	Contact Information	Demographic Data
	Communication Data	Health Data	National Identification Number
	Behavioural Data	Racial and/or Ethnic Data	Financial Data
Sensitivity	Normal	Sensitive	Special
Data subjects	Employees	Non-salaried staff	Ex-employees

The tab ‘Medew/HR gegevens’, which is short for employee HR data, gives (HR)managers access to complete employee records. In addition to using workflows, it’s also possible make changes to this record through workflows. It consists of:

- The basic personal data about the employee
- Their documents
- Their absences
- Their leaves
- Their (paid) salaries
- Their personal relationships
- Their reviews
- Their competences and education

- Their employment relationships
- Their expense claims
- Their activities and tasks
- Their digital file
- Their photos and signatures
- Their registered conversations

With all changes within workflows, institutions can add a free text field to give the user the option to add explanation to the change. There is also the option to add a document.

See 16.12 Loss of control through open text fields.
See 16.13 Lack of accuracy through manual registration of personal data.

4.3.5 Employment relationship management

Purposes	Employee administration		Salary and expense processing	
Data	Directly identifiable	Contact Information	Organisational Data	Financial Data
Sensitivity	Normal		Sensitive	
Data subjects	Employees		Non-salaried staff	Ex-employees

The tab 'Medew/Arbeidsrelatie', which is short for the employment relationship the employee has with the company relationship enables certain users to access and edit the employee's contract and different salary components. The salary components are all the different elements that make up the final salary for an employee, like base salary, bonuses, travel allowance, etc. Based on these components, an employee's salary gets calculated each payout period. Authorised users can generate a complete overview of the employee's salary and all the elements that went into calculating it and a payslip, which only includes the most important information. Institutions can decide what gets included on the payslip.

This section of HR2day also includes the details of the employee's contract, like the start date, vacation days and schedule. There are some free text fields to register the activities of the employee and special details about the employee.

4.3.6 Document management

Purposes	Employee administration		
Data	Directly identifiable	Financial	Organisational
	Demographic Data	National Identification Number	
Sensitivity	Normal	Sensitive	
Data subjects	Employees	Non-salaried staff	Ex-employees

All documents created and added in HR2day get added to the digital file, which is accessible under '*Medew/HR gegevens'*. This includes files saved during workflows and manually uploaded into the employee record, salary specifications sent to employees and

documents that have been added manually to the file. There are a basic version and an advanced version of the digital file manager.

With the advanced version, users can search in documents and add expiry dates. Users can add a deviating expiry date when they upload a file, which overrides the central expiry date. It's also possible to block users from accessing certain documents. For each document, the following data are registered:

- The creator of the document in HR2day
- The date and time it was created
- The module it falls under
- The category it falls under
- If it has one, the expiry date

There is a standard list of document categories, but employers can also create their own. It's possible for users to e-mail documents from HR2day to themselves.

4.3.6.1 SignRequest

HR2day facilitates the digital signing of documents, primarily employment contracts but also other HR-related documents, using SignRequest. Institutions can decide for themselves which documents they will have signed this way.

An HR Manager prepares a document within HR2day, which is then transmitted to SignRequest. SignRequest subsequently sends a private link to the data subject via email. After opening the link, the data subject is required to accept SignRequest's Terms of Service and Privacy Policy before viewing and signing the document. Once the document has been signed, the data subject receives an email confirmation and is provided with the opportunity to download a copy of the signed document for their records.

SignRequest uses multiple cookies and endpoints to facilitate this processing (see *Annex 1.3*). HR2day has not shared any further information about SignRequest. The responses to the DSARs (see 3.2.1 Data Subject Access Request) also have not provided clarity in this processing.

The majority of the end points found during our technical analysis on SignRequest reside outside the EEA (European Economic Area). SURF did not receive documentation on these endpoints nor the cookies. There was no Data Transfer Impact Assessment shared with SURF.

During the writing of this DPIA HR2day started replacing SignRequest with ValidSign (also a subsidiary of Visma).

See 16.9 Loss of control of subprocessors and recipients through lack of or incorrect agreements.

4.3.6.2 ValidSign

During the writing of this DPIA, system SignRequest was planned to be phased out in favor of system ValidSign. Due to the timing of this process, ValidSign has not yet undergone a technical analysis. This analysis will be conducted during follow-up testing of the system. However, a legal assessment of ValidSign has already been completed, and the findings can be found in 7.2.6 ValidSign.

4.3.7 Changing and storing user preferences

Purposes	Personalising the service	Providing the service and keeping it up-to-date	
Data	Technical Data		
Sensitivity	Normal		
Data subjects	Employees	Non-salaried staff	Administrators

Employers can select a default set-up for the panels of the EIC and the MIC, but employees can also set up the panels in a way they prefer. They also have the option to individually turn off notifications.
All user interfaces settings get stored through cookies, *see Tabel 18-4 for the list of cookies used by HR2day to store preferences*.

4.3.8 Generating reports

Purposes	Internal reports			
Data	Directly identifiable	Contact Information	Organisational Data	Health Data
Sensitivity	Normal	Sensitive	Special	
Data subjects	Non-salaried staff	Employees	Ex-employees	

It's possible to generate reports, analyses and dashboards based on all the data in HR2day. HR2day offers some standard reports. Employers can also customise their own reports and select exactly the (personal) data they want to include. Users have the choice to generate the reports in HR2day or in an Excel format.

4.3.9 Managing roles and profiles

Purposes	Providing the service and keeping it up-to-date		Securing the service	
Data	Directly identifiable	Contact Information	Organisational Data	
Sensitivity	Normal			
Data subjects	Non-salaried staff	Employees	Ex-employees	

The HR2day authorisation model is designed to manage and control access to sensitive HR data in a structured way. Access is derived from the users' organisational data. You start with nothing. This Role Based Access Control model consists of multiple layers:

1 Profile
Access is determined by user profiles, which define what actions (Create, Read, Update, Delete) a user can perform on each type of data (object) based on their job function (e.g., employee, manager, professional).

2 Organisation wide defaults
Organisation-wide default settings establish the baseline level of access for all users to each object.

3 Sharing rules
Sharing rules can be created manually or automatic through role-based sharing.

3a Manual sharing & ownership
Access can be further refined by manually sharing specific records or based on who owns the data. This option is used only when other options are not sufficient. When it's used, it's always for a very specific situation, concerning a very limited number of users.

3b Role based sharing
Role based sharing is the default in HR2day. Permissions are granted according to organisational roles, allowing users to access data relevant to their responsibilities.

The broadest access is provided through sharing rules, which can grant access to groups of users based on defined criteria.

Key points:
- **Organisational Structure:** Managers, by default, can access the data of employees they are responsible for and of any employees hierarchal beneath these employees. Hierarchical inheritance of access rights is on by default.
- **Functional Role:** Users can access data relevant to their functional role (such as absence management, leave, etc.).
- **Function:** Access is tailored to the user's job function.
- **Wider Access:** As you move through the layers, access becomes broader. Users get access to all personal data of all employees beneath them in the underlying vertical line of the hierarchy. While having the hierarchical inheritance of access rights functionality on, it's not possible to restrict this access to certain types of personal data, so a person would only have access to the types of personal data needed to perform their tasks.
- **Conflict Resolution:** If sharing rules conflict, the most permissive rule applies.

4.3.10 Logging

Purposes	Employee administration		Securing the service	
	Improving the service		Providing the service and keeping it up-to-date	
Data	Directly identifiable	Contact Information	Organisational Data	
	Communication Data	Technical Data		
Sensitivity	Normal			
Data subjects	Non-salaried staff	Employees	Ex-employees	Administrators

HR2day uses six types of logging. These logging options are offered by Salesforce as part of the platform functionality:

- Login history (inloghistorie)
- Event monitoring (logboek van acties)
- Change history tracing (historietracing)
- Error logging (foutopsporingslogboeken)
- Setup audit trail (logboek van instellingswijzigingen)
- Email logs (emaillogboekbestanden)

HR2day has stated that this is all logging they perform. SURF has no information on logging by their sub-processors other than Salesforce and Expo.

4.3.10.1 Salesforce

According to HR2day, Salesforce probably has a form of monitoring logging for security purposes but HR2day does not have access to it nor shared information about this logging.[23] SURF did find information on logging by Salesforce scattered through their documentation. However, there is no clear picture of what is applicable to HR2day's situation since the documentation of Salesforce applies to more or all their services.

Salesforce states in their '*The Salesforce Platform - Transformed for Tomorrow*' document they collect data as one of their architectural principles:

> *"Integration of all services into a standard observability platform for efficient monitoring, which includes log collection, metrics gathering, alerting, distributed tracing, and tracking of service operations like traffic volume, error rates, and resource utilization."*[24]

SURF did not receive information about the collection of logging data by Salesforce through the DSARs, nor is there clear documentation on how Salesforce performs logging for their purposes. HR2day provided a document explaining the distinction Salesforce makes between Customer Data (all data entered into the application by or on behalf of customers, including personal data of employees of HR2day's end customers) and Usage Data (data generated by the use of the platform, for operational, security and analytical purposes). The most detailed available description of the Usage Data Salesforce collects is:

> *"Salesforce may track and analyze the usage of the Covered Services for the purposes of security and helping Salesforce improve both the Covered Services and the user experience in using the Covered Services. For example, we may use this information to understand and analyze trends or track which of our features are used most often to improve product functionality."*[25]

[23] E-mail from HR2day, 15 May 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, accessed on 23 January 2026.

Any identifying information in the Usage Data gets anonymised before Salesforce employees get access to it.[26] Therefore, Salesforce states that the Usage Data gets processed in a way that doesn't make it possible to identify individuals.[27] HR2day has not provided the anonymisation methods Salesforce uses to anonymise the personal data collected as Usage Data, any contractual agreements binding Salesforce to their commitments or an exhaustive list of specific data fields Salesforce collects. Therefore SURF has not been able to verify that Salesforce doesn't process personal data when collecting usage data.

4.3.10.2 Login history

Purposes	Securing the service			
Data	Directly identifiable		Contact Information	
	Organisational Data		Technical Data	
Sensitivity	Normal			
Data subjects	Non-salaried staff	Employees	Ex-employees	Administrators
Retention period	6 months			
Access	System administrator			

This log displays details about the users' login history and is used for securing the service, such as monitoring suspicious activity. The log can be accessed and viewed through the HR2day interface and downloaded as a .csv file (comma separated values).

Data Subject Access Request
All data generated in this log during our test was included in the dataset provided to us by HR2day following our submission of a Data Subject Access Request.

4.3.10.3 Event monitoring

Purposes	Securing the service			
Data	Directly identifiable		Contact Information	
	Organisational Data		Technical Data	
Sensitivity	Normal			
Data subjects	Non-salaried staff	Employees	Ex-employees	Administrators
Retention period	3 days[28]			
Access	System administrator			

Event logging has been implemented to keep record of six types of events. These events are tracked to secure the service. Event logs help detect suspicious activities and potential breaches by recording user actions, logins, and system events, enabling quick identification and response to threats.

[26] Email from HR2day contractor, received on 22 January 2026.

[27] Uitleg van de verwerking van data door Salesforce by HR2day, received on 2 January 2026.

[28] The Apex Unexpected Exceptions log is kept indefinitely after the data has been anonymised. See 5.4.1 for more information on the anonymisation.

Type event logging	Description
Login	This overview shows details about the login history of users and is used for security purposes, such as monitoring suspicious activities.
Logout	This shows details of user sessions that end. The purpose is to support security measures.
Hostname Redirects	This overview displays details of both blocked and successful redirects during login. Redirects may occur due to changed naming; if not updated in HR2day's code or users' bookmarks, users cannot log in. Detecting this allows it to be resolved either in the HR2day code or by contacting users to update their bookmarks.
CSP Violation	This overview shows details of blocked requests on Lightning Experience pages. It provides insight into whether there are attempted hacking attempts on HR2day within the Salesforce platform.
API Total Usage	Gives details about API requests. The purpose is to have insight into the usage of APIs in an environment.
Apex Unexpected Exceptions	Reports errors in Apex code in HR2day/Salesforce so they can be resolved and the software improved.

Tabel 4-2, the six types of event logging.

The personal data processed in these types of event logging can be reviewed in *Tabel 18-9, processed personal data in event logging on login*.

Data Subject Access Request
All data generated in these logs during our test (3.2.1 Data Subject Access Request) was **not** included in the dataset provided to us by HR2day following our submission of a Data Subject Access Request.

4.3.10.4 Change History Tracing

Purposes	Securing the service			
Data	Directly identifiable		Contact Information	
	Organisational Data		Technical Data	
Sensitivity	Normal		Sensitive	
Data subjects	Non-salaried staff	Employees	Ex-employees	Administrators
Retention period	24 months			
Access	System administrator			

Change History Tracing allows logging who changed which field and when, including the previous value. The purpose is to provide the institution (customer) with evidence for internal controls and external audits (e.g., accountants) to show who made what changes and when.

There is a limit to 20 fields max per object where *change history tracing* can be enabled. By default, HR2day has enabled the following 17 objects:

- 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

The institution/customer can, through their system administrator, change on what fields *change history tracing* is enabled.

Data Subject Access Request
All data generated in this log during our test (3.2.1 Data Subject Access Request) was included in the dataset provided to us by HR2day following our submission of a Data Subject Access Request.

4.3.10.5 Debug Logs

Purposes	Improving the service	Providing the service and keeping it up-to-date		
Data	Directly identifiable			
	Organisational Data	Technical Data		
Sensitivity	Normal			
Data subjects	Non-salaried staff	Employees	Ex-employees	Administrators
Retention period	7 days			
Access	System administrator			

With debugging logs, HR2day can check where things go wrong when a user receives an error message. The purpose is to resolve these errors and thereby improve the system. For a user, logging of their transactions is disabled by default. The debugging logs are kept for 7 days and then automatically deleted by Salesforce.

[29] With the introduction of Validsign as replacement for SignRequest this will change.

The log contains the following fields per event:
- Execution Units
- Code Units
- Log Entries
- Timestamp
- Event Indicator
- Cumulative Resource Usage
- Cumulative Profiling Information
- API Version
- Log Category
- Log Level

Data Subject Access Request
This log keeping was not enabled in the test environment thus no data was generated in this log during our test.

4.3.10.6 Setup Audit Trail

Purposes	Securing the service	
Data	Directly identifiable	Contact Information
	Organisational Data	Technical Data
Sensitivity	Normal	Sensitive
Data subjects	Administrators	
Retention period	6 months	
Access	System administrator	

Setup audit trail is a feature in Salesforce that automatically records all configuration changes. It tracks which user made what changes and when in the settings of your Salesforce environment. This logging is used to have an audit trail to detect unauthorised changes to the system's settings, it also generates a full history of the system configuration.

The log contains the following fields per event:
- User
- Timestamp
- Type of change
- Details
- IP address
- Session information

- User who made the change
- Time of the modification
- Type of change (for example: new field, workflow adjusted)
- Details of what was changed exactly
- IP address from which the change originated
- Session information

Data Subject Access Request
All data generated in this log during our test (3.2.1 Data Subject Access Request) was **not** included in the dataset provided to us by HR2day following our submission of a Data Subject Access Request.

4.3.10.7 Email Logs

Purposes	Securing the service			
Data	Directly identifiable		Contact Information	
	Organisational Data		Technical Data	
Sensitivity	Normal		Sensitive	
Data subjects	Non-salaried staff	Employees	Ex-employees	Administrators
Retention period	30 days			
Access	System administrator			

Email Logs are used to determine the status of email delivery. If sending was unsuccessful, an error code is also available indicating why the sending failed.

Annex 1.5 has a full list of data being processed for this logging activity.

Data Subject Access Request
All data generated in this log during our test (3.2.1 Data Subject Access Request) was **not** included in the dataset provided to us by HR2day following our submission of a Data Subject Access Request.

4.3.11 Finger printing, intrusion detection

Purposes	Securing the service			
Data	Directly identifiable		Technical Data	
Sensitivity	Normal			
Data subjects	Non-salaried staff	Employees	Ex-employees	Administrators

HR2day and third parties collect personal data by placing cookies in users' browsers. For a complete list of all cookies and purposes, see *appendix 1.4*.

- Finger printing
- Authenticeren
- Intrusion detection by Salesforce

HR2day uses the following cookies for Security purposes, these cookies are used to create a fingerprint of the datasubject:

Cookie name	Age	Description
79eb100099b9a8bf	Session	Browser Fingerprint trigger cookie. Used to detect session security problems.
52609e00b7ee307e	Session	Browser Fingerprint cookie. Used to detect session security problems.
__Host-ERIC_PROD-<random number>	1 Minute	Enterprise Request Infrastructure Cookie (ERIC) carries the CSRF security token between the server and client. Name indicates server mode (PROD/PRODDEBUG) and a random number. Different token for each Lightning app.

__Host-ERIC_PRODDEBUG-<random number>		Enterprise Request Infrastructure Cookie (ERIC) carries the CSRF security token between the server and client. Name indicates server mode (PROD/PRODDEBUG) and a random number. Different token for each Lightning app.
clientSrc	Session	Used for security protections.

Tabel 4-3, cookies used in finger printing and/or intrusion detection.

4.4 Disclosure

4.4.1 E-mailing

Purposes	Employee administration	Internal reports	
Data	Directly identifiable Data	Contact Information	Demographic Data
	Organisational Data	Health Data	Financial Data
Sensitivity	Normal	Sensitive	Special
Data subjects	Employees	Non-salaried staff	Ex-employees

Users can e-mail copies of documents and excel versions of reports, they have access to, to themselves.

HR2day also sends a newsletter to super users and other users who have registered themselves.

4.4.2 Downloading

Purposes	Employee administration	Internal reports	
Data	Directly identifiable Data	Contact Information	Demographic Data
	Organisational Data	Health Data	Financial Data
Sensitivity	Normal	Sensitive	Special
Data subjects	Employees	Non-salaried staff	Ex-employees

Users can download documents, reports and logging records from HR2day's user interface.

4.4.3 Receiving notifications

Purposes	Personalising the service	Employee administration
Data	Directly identifiable Data	Contact Information
	Organisational Data	Demographic Data
Sensitivity	Normal	
Data subjects	Employees	Non-salaried staff

The HR2day+ app can receive notifications, these notifications are alerts on certain changes or signals. HR2day uses an automated notification mechanism that informs employees and managers of activities that require attention.

Employees receive notifications for newly available documents (such as payslips and annual statements), leave approvals or rejections, declaration submissions and status updates, process management decisions (approval/disapproval) and general system announcements.

Managers receive notifications concerning pending leave requests, general changes awaiting approval, declaration and professionalisation submissions from their team members.

Each notification carries a preset title, for example: “A new payslip is available” or “A new annual statement is available”. These notifications typically include a notification body containing personal data elements such as the employee’s name, relevant dates (leave start/end dates), document identifiers (declaration numbers), approval status and reasons for rejection (afwijzing). Document file names might reveal personal information.

Notifications are enabled by default and users can individually control notification preferences since the app prompts the user whether they want to receive notifications. There is no granular control for user to define what notifications to receive or not.

The detailed specifications of all notification types, triggering conditions and data elements transmitted are documented in 0 HR2day App Push Notifications.

The app uses Expo as a sub-processor for processing these notifications. Notifications are sent through Expo's push notification service, which requires the app to register the device and obtain a unique token for each device.

Expo will delete the push notification payload after it has been shared with Google or Apple[30]. Notifications are stored only in memory and in message queues, not in databases.

Expo itself is a US based cloud service, and data may be processed in various data centres, depending on the service architecture and the location of the users.

The metadata that will be stored by Expo, in this case:

- Push Tokens, these are persistent identifiers linking to individual devices and must be retained for the service to function.
- Push Receipts, recording which notifications were successfully delivered to Google/Apple.
- Audit Logs, records of delivery attempts and status.
- User device information, crash traces and IP address.

The metadata will be processed for the term of the agreement, or as otherwise

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

required by law or agreed between the parties.[31] Expo uses user device information for aggregate trend analysis.[32]

4.4.4 Processing support requests

Purposes	Providing customer support		
Data	Directly identifiable	Contact Information	
	Communication Data	Organisational	
Sensitivity	Normal		
Data subjects	Employees	Non-salaried staff	Ex-employees

Only super users can submit support requests through tickets in the 'Klantportaal' (customer portal). In some exceptional cases, they also call or email HR2day. In the Klantportaal, they can enter:

- Subject of the request
- Description of the request in a free text field
- Attachment

4.4.5 Proxy login (inloggen als)

Purposes	Providing customer support		
Data	Directly identifiable	Contact data	Demographic data
	Communication Data	Organisational data	Health data
	Financial data	Trade union data	Political data
Sensitivity	Normal	Sensitive	Special
Data subjects	Employees	Non-salaried staff	Ex-employees

HR2day provides functionality referred to as **'inloggen als / login as access'**, which enables authorised administrative users of the controller to temporarily assume the identity of another user within the system. When this mode is enabled, the administrator experiences the system exactly as the impersonated user would, including full access to their interface, permissions, and personal data.

Activation of this functionality is at the discretion of the institution, and HR2Day does not enforce or configure this feature by default. The feature includes only limited logging. It records when an administrator starts and ends an impersonation session (4.3.10.6 Setup Audit Trail), but actions performed during that session are logged as if executed by the impersonated user (4.3.10.4 Change History Tracing). Viewing or read-only activities are not logged.

[31] Data processing agreement Expo and HR2Day - Expo DPA - 2025.pdf

[32] Data processing agreement Expo and HR2Day - Expo DPA - 2025.pdf

5 Techniques and methods of processing

5.1 Search

The search functionality in HR2day uses Einstein search, which is an AI solution on the Lightning platform.[33] It enables users to:

- "Receive personalized results based on how you work in Salesforce.
- See instant suggested records and previews when you start typing.
- Enter a term, and search generates a recommended result.
- Use common words and phrases in the search bar and get relevant information."[34]

For certain features of Einstein search, it uses:

- Customer Data and salesforce objects, and/or
- Usage data.

These data can be processed in and be used to train global models. Global models are predictive models trained by data from multiple customer organisations of Salesforce.[35] It's possible to opt out of providing training data to the global models, while still being able to use the Einstein search functionality.

Product	Feature	Customer data and Salesforce objects used	Usage data used	Global model used
Einstein Search	Einstein AI-Generated Search Answers	Knowledge	Knowledge search terms, knowledge search results (record IDs, query and document matching metadata), and knowledge article metadata.	No
	Einstein Search	N/A	Search terms, search results (record IDs, query and document matching metadata, and user-MRU and document matching metadata), and org metadata. See How Does Einstein Search Use My Data.	Yes

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

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

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

	Einstein Search for Knowledge	N/A	Knowledge search terms, knowledge search results (record IDs, query and document matching metadata, and user-MRU and document matching metadata), and knowledge article metadata. See Enable Einstein Search for Knowledge.	Yes

A search query wasn't part of the testing scenarios performed in HR2day, so Einstein Search falls outside of the technical testing scope. SURF assumes institutions will opt out of providing training data to global models.

5.2 API

HR2day uses the Salesforce REST API to connect their Salesforce instance programmatically with other internal or external systems. The REST API provides an interface for accessing virtually everything that can be done via the native UI. Customers send requests to specific resource URIs to access, manipulate, search, query data, metadata, and other resources within the application.

This Salesforce Integration Platform uses MuleSoft to facilitate the management of automated processes, ensuring seamless data flow and connectivity between Salesforce and custom or third-party services. This ensures universal connectivity support for standard API specifications like OpenAPI for synchronous and AsyncAPI for asynchronous interactions.

Customers (HR2day or Institutions?) can use resources like the Portability resource via the REST API to compile and locate customers' personally identifiable information (PII) across records for data portability requests.

In the Salesforce API documentation[36] and in the The Salesforce Platform documentation[37] is specified that the data visibility is user specific. The data that can be accessed or manipulated through the API is subject to the same security and sharing controls that apply to that user within HR2day.

5.3 Cookies

Cookies are small text files that are placed on a device when visiting HR2day, these cookies are used to store (personal) data on the user's device.

Cookies in a service like HR2day can be used to:
- maintain secure user sessions
- remember user preferences and settings across visits
- enable seamless authentication and authorisation
- collect analytics for service improvement

[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).

- obtaining and managing user consent
- collect analytics for service improvement

HR2day uses cookies to support its services: 6 cookies by HR2day, 33 cookies by Salesforce, 6 cookies by SignRequest and 1 cookie from an unknown 3rd party (MyFonts.net).

The cookie statement[38] shared by HR2day was only applicable on its public/commercial website.

HR2Days' cookie statement did not document any cookies used by their SaaS application. The documentation of the cookies placed by HR2day[39] was provided by technical staff of HR2day upon request.

Upon request HR2Day was able to produce documentation of a selection of cookies placed by Salesforce[40].

To get the full documentation of all cookies placed by Salesforce HR2Day had to file a support request with Salesforce. The documentation of the leftover cookies was provided after contact with Salesforce support by HR2day staff.

All cookies used by HR2day are functional (required) cookies and therefore there is no consent mechanism in place (cookie banner).

Validsign has been introduced after our technical analysis as a replacement for SignRequest. Because of this the cookies used by Validsign have not been included in this assessment.

Refer to Annex 1.4 Cookies for a full list of used cookies.

For more see *16.4 Loss of control due to lack of transparency about processing* of personal data through cookies.

5.4 Anonymisation

According to *The Salesforce Platform documentation*[41] logs are being anonymised, however it doesn't specify what data is logged and how it is being anonymised. This follows our findings in paragraph 4.3.10.1 Salesforce.

5.4.1 Apex Unexpected Exceptions Logging

The Apex Unexpected Exceptions Logging data will be stored anonymously. This is done by stripping the user data from the logs. The fields USER_ID and USER_ID_DERIVED are being stripped from this data set.

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

[39] Refer to Annex 1.4 Cookies for a full list of used cookies.

[40] Cookie documentation published on Salesforce Help - https://help.salesforce.com/s/articleView?id=xcloud.platform_cookies.htm&type=5

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

5.5 Pseudonymisation

No documentation on pseudonymisation was given and HR2day has stated it does not have this functionality.[42]

5.6 Test environment

HR2day provides a feature in the test-environment of HR2day to create fake employees so that tests and accepting of changes to the system can be done without using personal data and unnecessary duplicates must be made.

5.7 Data Encryption

HR2day relies on Salesforce for security and is therefore also the provider of encryption service. Salesforce has a Zero-Trust Security principle where it states that encryption of data both in transit and at rest is implemented as part of their defence strategy.

Data in transit

Salesforce uses industry-accepted end to end encryption products to protect Customer Data and communications during transmissions between a customer's network and the Salesforce services, as well as within the Salesforce infrastructure domains through Transport Layer Encryption (TLS)[43]. Salesforce requires TLS 1.2 as the minimum protocol version for its core services, and newer services and regions increasingly support TLS 1.3 as well. TLS 1.2+ is enforced for both external client connections and Salesforce-initiated connections (APIs, callouts, etc). Older protocols like TLS 1.0/1.1 are no longer supported..

Data at Rest

HR2Day shared the C5 ISAE report on Hyperforce which states that Salesforce encrypts the data at rest. Hyperforce leverages AWS storage resources configured with encryption enabled by default, utilising Customer-managed Keys (CMK) through AWS Key Management Services (KMS). Salesforce manages these keys on behalf of HR2Day, including the annual rotation process.

Salesforce offers additional encryption options through its Salesforce Shield[44] service, which is specifically designed to add extra protection for sensitive data and special categories of personal data. However, HR2Day does not use these enhanced encryption levels. As a result, sensitive and special category data are not protected with cell-level encryption.

AWS[45]

The Customer Data is also encrypted at rest. For the purposes of preventing fraud or abuse and to comply with applicable law, hosting provider AWS reserves the ability to access systems processing and storing encrypted Customer Data.The Customer Data is also

[42] Communication HR2day 10 July 2025.

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

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

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

encrypted at rest. For the purposes of preventing fraud or abuse and to comply with applicable law, hosting provider AWS reserves the ability to access systems processing and storing encrypted Customer Data.

Salesforce has implemented technical measures that prevent AWS from accessing unencrypted Customer Data and from accessing encryption keys used to encrypt Customer Data. With Platform Encryption, customers may generate and store encryption key material outside of Salesforce.

5.8 Back-up

Backup policies and procedures are documented and communicated in accordance with C5 control SP-01, establishing clear requirements for data backup frequency and recovery objectives, Recovery Time Objective of 12 hours and a Recovery Point Objective of 4 hours[46]. Backup data is maintained in encrypted form using encryption standards. Access to backed-up data and execution of restore operations is restricted to authorised personnel only. Salesforce manages the encryption keys.

Recovery procedures are subject to regular testing and validation to ensure the integrity and recoverability of backup systems.

The shared documentation does not specify what encryption method is used by salesforce for data rest on Hyperforce, besides it being state-of-the-art. According to the C5 ISAE there are no deviations on the associated controls.

[46] Disaster Recovery Testing Summary Salesforce Hyperforce Infrastructure – February 2024 / January 2025 – opened on 20 – 01 – 2026

6 Legal and policy framework

6.1 General contractual framework

HR2day gets most of their customers through tenders. Each institution determines their own, individual requirements for the product they want and the contracts the vendor has to accept. This means HR2day has slightly different contracts for each customer. Based on a sample of contracts for different customers, the necessities for a functioning contractual framework and HR2day's role as a processor, this DPIA assumes each customer of HR2day has at least a service agreement (including a description of the tendered services if applicable), a service level agreement and a processor agreement based on:

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

HR2day also has general terms and conditions that apply to the use of their product. However, the applicability of these has been excluded in the contracts from the sample and they have been replaced by the ARBIT conditions. HR2day confirmed that this is the case for all SURF-members.

As mentioned, HR2day has a processor agreement with every customer, in which they commit to only processing the personal data in HR2day as needed to provide the services as described in the service agreement, and not to process these data for their own purposes.[49] The main purposes mentioned are personnel administration and payroll administration.

6.2 Applicable laws and policy

This paragraph contains a non-limitative list of laws, policy and rules that may apply to the processing activities that happen in HR2day:

Abbreviation	Legal or policy framework	Relevant articles (optional)	Relevancy for users HR2day
AWR	General Act on National Taxes (Algemene Wet inzake Rijksbelastingen)	Art. 52(4)	Retention period for certain taks data
	Working Conditions Decree (Arbeidsomstandighedenbesluit)	Various articles	HRM legislation
Arbowet	Working Conditions Act (Arbeidsomstandighedenwet)	Art. 3 and 18	HRM legislation

[47] https://www.surf.nl/files/2019-04/SURF-Model-Verwerkersovereenkomst-3.0.pdf, accessed on 14 May 2025.

[48] https://www.surf.nl/surf-juridisch-normenkader-cloudservices, accessed on 14 May 2025.

[49] Art. 2.3 Template Verwerkersovereenkomst HR2day.pdf

	Working Hours Act (Arbeidstijdenwet)		HRM legislation
AW	Archives Act 1995, including Archives Decree 1995 and Archives Regulations (Archiefwet)	Art. 5	Legal basis selection lists
	Selection list of colleges/universities/vocational colleges (selectielijsten)	N/A	Retention periods for data that falls under the AW
	Policy rules processing personal data health sick employees (Beleidsregels verwerking persoonsgegevens gezondheid zieke werknemers)	N/A	Rules regarding the processing of personal data about sick employees
BW	Civil Code Book 7	Art. 7:611 and Art. 7:400 et seq.	Rules for behaviour between employees and employees
	Information security policy	N/A	Policy regarding security practices
	Privacy policy of the institution	N/A	Policy regaring privacy practices
Tw	Telecommunications Act (Telecommunicatiewet)	Various articles	Rules for cookies and similiar technologies
	Wage Tax Implementation Regulation 2011 (Uitvoeringsregeling loonbelasting 2011)	Art. 7.5(4) and 12.1(5)	Identification duty and retention period wage tax statement
UAVG	GDPR Implementation Act	Various articles	Dutch implementation of the GDPR
Wabb	General Provisions Act on Citizen Service Numbers (Wet algemene bepalingen burgerservicenummer)	Articles 10, 11, 12 and 13	Rules regarding the processing of national identification numbers
Wfsv	Social Insurance Funding Act (Wet financiering sociale verzekeringen)	Various articles	Rules on national insurance

	Wage Tax Act 1964 (Wet op de loonbelasting 1964)	Art. 28	Tax rules
WOR	Works Councils Act (Wet op de ondernemingsraden)	Art. 27(1)	Rules on works councils' rights
Wvp	Gatekeeper Improvement Act (Wet verbetering poortwachter)	Various articles	Rules on long-term sick leave

7 Concerned parties

This chapter will describe the different parties involved in the data processing in HR2day and their roles.

The GDPR contains definitions of the different roles of parties involved in the processing of data:
(joint) controller, processor and subprocessor. Article 4(7) of the GDPR defines the (joint) controller as:

> *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."*

Article 26 of the GDPR stipulates that where two or more data controllers jointly determine the
purposes and means of a processing, they are joint controllers. Joint controllers must determine
their respective responsibilities for compliance with obligations under the GDPR in a transparent
manner, especially towards data subjects, in an arrangement between them.

Article 4(8) of the GDPR defines a processor as:

> *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."*

A subprocessor is another processor engaged by a processor that assists in the processing of
personal data on behalf of a data controller.

Article 28 GDPR sets out various obligations of processors towards the controllers for whom they
process data. Article 28(3) GDPR contains specific obligations for the processor. Such obligations
include only processing personal data in accordance with documented instructions from the data controller and cooperating with audits by a data controller. Article 28(4) GDPR stipulates that a data processor may use subprocessors to perform specific tasks for the data controller but only with the prior authorisation of the data controller.

When data protection roles are assessed, the formal contractual division of roles is not leading nor decisive. The actual role of a party must primarily be determined on the basis of factual
circumstances. Therefore, SURF takes these circumstances into account when determining the data protection roles in DPIAs.

7.1 Institutions as data controllers and HR2day as processor

HR2day has processor agreements with all their customers, indicating that the institutions as customers are data controllers for the processing activities described in the processor agreements (see 2 Purposes). Since institutions determine the purposes and means for all personal data they put into and process in HR2day in the context of their payroll and personnel administration, they are controllers for these processing operations. The processing operations have been described in chapter 4. Some processing activities constitute data transfers, which are described in chapter 9. HR2day is processor for the processing operations described in the processor agreements.

7.2 Subprocessors

The subprocessors mentioned in HR2day's processor agreement are:

Name	Processing activities	Personal data
Salesforce	Salesforce manages, maintains and develops the platform (force.com) on which HR2day has been developed and is made available.	All personal data being processed in and via HR2day
SignRequest	SignRequest is a provider of the solution for electronically signing agreements.	Digital signature data
Workbee	Workbee is the 'broker' that ensures that the (absenteeism) data from HR2day is sent to the occupational health and safety service contracted by the data controller.	Absence data
Infor	Infor is the supplier of the HR Analytics solution in which personal data is also stored for reporting purposes.	All personal data in the HR2day application

Additionally, the technical research and conversations with the vendor showed that HR2day uses two more subprocessors that aren't mentioned in the processor agreements with the institutions.

Name	Processing activities	Personal data
Expo	Expo enables the sending of notifications in the mobile HR2day+ app.	Unknown

ValidSign	ValidSign is a provider of the solution for electronically signing agreements.	Digital signature data

7.2.1 Salesforce

Salesforce provides the force.com platform which contains the HR2day application. HR2day has a Platform Solution Reseller Agreement (PSRA) with Salesforce Inc., where HR2day is the Reseller. Salesforce Inc. is established in San Francisco in the United States. The generic Salesforce Data Processing Addendum is attached to this agreement and applies to the data processing Salesforce does as a sub-processor. After an amendment to the PSRA, the DPA from revision date 2023 is the applicable version.[50] This processor agreement only applies to Customer Data, which Salesforce defines as:

> *"...all electronic data or information submitted by a Customer to SFDC's systems which is accessible to the Customer through the Combined Solution while resident on SFDC's systems."*[51]

HR2day hasn't given Salesforce any additional contractual instructions about processing personal data and there are provisions in the DPA about Salesforce processing any of the personal data that is covered by the DPA for its own purposes. According to Salesforce, the company has no visibility into the content of Customer data.[52]

Salesforce processes personal data:

> *"...only on behalf of Reseller and in accordance with Reseller's documented instructions including those conveyed on behalf of the applicable Customer) and/or a Customer's instructions, as the case may be, for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by Reseller (including those conveyed by or on behalf of the applicable Customer (e.g., via email)) where such instructions are consistent with the terms of the Agreement."*[53]

The DPA defines personal data as:

> *"...any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is Customer Data."*[54]

[50] https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/no-index/reseller-dpa.pdf

[51] Article 11.4 of the Platform Solution Reseller Agreement between Salesforce and HR2day.

[52] Email from Salesforce, 17 Juli 2025.

[53] Article 2.2 of the Salesforce DPA.

[54] Article 1 of the Salesforce DPA.

This means that the purpose limitation of article 2.2 only applies to personal data that are part of the Customer Data.

According to Schedule 2 of The Data Processing Addendum, it applies to, among others, Users of the Services and to personal data including names, titles and professional life data, as well as special categories of personal data. The list of data subjects and personal the DPA applies is non-exhaustive.

Salesforce provides a list of their sub-processors in their 'Salesforce Infrastructure and Sub-processors' document. This list includes the locations where Salesforce processes and/or stores data for each sub-processor. One of Salesforce's sub-processors for HR2day is AWS, since the platform HR2day runs on is entirely hosted on AWS infrastructure. To get notified of Salesforce's new sub-processors, you need to subscribe to get notifications.[55]

7.2.2 SignRequest

HR2day has a service agreement and sub-processor agreement with SignRequest B.V., which is established in Amsterdam, The Netherlands. However, users also must accept SignRequest's privacy statement and terms and conditions when they want to use the contract signing functionality that SignRequest provides.

7.2.3 Workbee

HR2day has a service agreement and a subprocessor agreement with Workbee B.V. Workbee is established in Hilversum, The Netherlands.

7.2.4 Infor

HR2day has a service agreement and subprocessor agreement with Infor (Barneveld) B.V.

7.2.5 Expo

During the testing, SURF discovered that HR2day uses Expo to send notifications to users. HR2day shared the Data Processum Addendum it has concluded with the US-headquartered 650 Industries Inc. (Expo). According to an online source, 650 Industries Inc. is established in Palo Alto, California, but SURF has not been able to verify this.[56]

7.2.6 ValidSign

ValidSign B.V. is a subprocessor that HR2day has been phasing in while this DPIA was being conducted. SURF hasn't been able to include it in the technical tests. HR2day does have a valid service agreement and sub processor agreement with ValidSign.

7.3 Recipients

All of the subprocessors described in 7.2 can be qualified as recipients. When institutions and HR2day are legally compelled to disclose personal data to governmental authorities, these are also recipients.

[55] Subscribe to notifications of new Sub-processors, https://www.salesforce.com/form/other/trust-compliance/?d=pb, accessed on 14 October 2025.

[56] https://www.verif.com/en/company/650-Industries-Inc--68d9b5d212992303386247ce/, accessed on 23 January 2026.

Additionally, there were some end points found with which data was exchanged during the test scenarios. An end point is any device, service, or application connected to a network that can send or receive data. In this case, these are endpoints that are involved in the communication during the technical research. SURF has been able to connect the engagement of the following end points to the use of the SignRequest services. However, it's not clear what data are exchanged and if this includes personal data from users.

- 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

The subprocessor agreement with SignRequest does not include any subprocessors.

Another recipient of personal data is Google. HR2day uses the Google Maps integration to calculate the travel distance for employees and shares their addresses with Google to that end. Google should only process these data for this purpose, but there is no service agreement or subprocessor agreement with Google. Therefore, it's unclear if Google processes these data for its own purposes.

The HR2day+ app can be installed via the Apple App Store and the Play Store. As a result, Apple and Google have a link between the use of the HR2day+ app and the user's Apple and Google account. This is not specific to the HR2day+ App, but applies to all apps offered via the Apple App Store. HR2day hasn't shown processor agreements with Apple and Google.

7.4 Other controllers

7.4.1 HR2day

HR2day states that the company only processes personal data obtained from customers in its capacity as a processor and therefore does not process this data for purposes and through means it determines itself.

However, HR2day's privacy statement shows that HR2day processes:

- "Personal basic information such as name, address, telephone number, email address and demographic information
- Information relating to the user and web traffic such as login details, username and IP address
- Content that you have uploaded or provided such as photos, comments, articles and videos
- Statistics that show how users use our software and the consent we offer."[57]

These personal data are being collected directly from persons working for their customers and when users are using the website, which can be users of the HR2day application. It is unclear if these data are being collected for the purposes mentioned in the privacy statement, or if HR2day carries out processing activities with personal data originally collected for the institutions' purposes through the application.

The data are being used – among other things – for the following purposes:

- "Improving and (further) developing the quality, functionality and user experience of our products, services and the HR2day website
- Providing customer support for our products and services
- Detecting, remedying and preventing threats to and misuse of security, performing maintenance and removing bugs
- Managing marketing preferences and directing marketing content
- Creating interest profiles for promoting relevant products and services (profiling)"[58]

These purposes have not been described in the processor agreements. The fact that these personal data and purposes are mentioned in the HR2day privacy statement is also an indication that the institutions haven't instructed HR2day to carry out these processing activities.

User satisfaction
HR2day collects user satisfaction reviews through pop-ups in the application for service improvement. Users get the pop-ups once every six months. If they ignore it, it returns after two months and if they reply, it returns after six months. They can give the application a rating and leave a comment. HR2day decides which data to collect and stores these data with the e-mail address of the user for three years. Institutions aren't able to turn off this functionality, access these data or influence what HR2day collects. After three years, the e-mail address is removed from the review. These reviews aren't part of the processing agreements with the institutions and institutions have no way to instruct HR2day about this processing. Therefore, HR2day has to be qualified as a controller for this.

7.4.2 Salesforce

Salesforce is the owner of the Lighting platform, an integral part of the HR2day product, and has its own privacy statement. This statement only applies when Salesforce processes

[57] Privacyverklaring HR2day, consulted on 18 May 2025.

[58] Privacyverklaring HR2day

personal data as a controller, not to personal data submitted voluntarily to their services as an authorised user. Since the Salesforce DPA doesn't contain any clauses about Salesforce being allowed to process the data it processes as processor for its own purposes, the privacy statement shouldn't cover any personal data that is covered by the DPA.

According to the privacy statement, Salesforce may collect information about users' devices and their usage of Salesforce's services through log files and other technologies, some of which may qualify as personal data (including Usage Data) as a data controller when users use and interact with their products and services.[59] Since Lightning platform is one of Salesforce's services, this situation applies to HR2day. When Salesforce collects personal (logging) data in this manner, it processes these for its own purposes as controller. These purposes include developing and deploying AI systems and combining the personal data with personal data gathered from other sources. In other documentation, Salesforce states that it may track and analyse the usage of the service for purposes of security and service improvement.[60] HR2day has provided an overview of the logging they instructed Salesforce to carry out using their functionality. It is unclear if this logging and the tracked usage data fall under the definition of Customer Data and are covered by the Salesforce DPA or not. Based on the purposes stated in the privacy statement, it can be assumed Salesforce processes more logging data than the types provided in the HR2day documentation as controller. It is unclear what this processing entails and what personal data it may contain. According to Salesforce, they process the Usage Data in a way that doesn't make it possible to identify individuals (see 4.3.10.1 Salesforce).

Salesforce also uses a number of cookies to collect personal data, which aren't covered in the DPA and for which there isn't public documentation available. It is unclear if some of the purposes of these cookies exceed the purpose of providing the Salesforce's services. Due to the lack of transparancy, institutions have no way to – through HR2day – approve the use of these cookies and to instruct Salesforce about the use of these cookies.

[59] Full Salesforce Privacy Statement, https://www.salesforce.com/company/legal/privacy/#privacy-statement, accessed on 15 October 2025.

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

8 Interests in the data processing

8.1 Educational and research institutions

These institutions have an interest in having an HR and payroll system that enables them to carry out their legal obligations as employers: which include data protection obligations: and supports the effective, efficient and safe functioning of their business operations. They also have a financial interest in preventing enforcement by legal authorities and an interest in protecting their reputation as trustworthy institutions.

8.2 HR2day

HR2day is being used by approximately 15-20 universities of applied sciences and approximately 5-10 vocational colleges. The company has a commercial interest in maintaining and expanding this market share by providing reliable and high-quality services, among other things. Additionally, it has an interest in complying with laws and regulations like the GDPR and having a reputation as a trustworthy HR and payroll services provider.

8.3 Sub-processors

Sub-processors have a commercial interest in keeping HR2day, by providing quality services and enabling the company to comply with laws and regulations. They also have their interest in complying with laws and regulations and protecting their reputation.

Salesforce, as the sub-processor that hosts the entire HR2day application is an especially important sub-processor to HR2day. Salesforce does have a commercial interest in retaining HR2day as a customer. However, due to its massive size and global reach, Salesforce's dependence on HR2day as a customer is much smaller than the other way around.

8.3.1 Apple and Google

As described in paragraph *1.4 HR2day+ App,* Apple and Google are involved as possible sub-processors for the mobile app. Apple and Google are involved as distributors of the mobile app via their app stores, where data processing takes place within their own commercial frameworks and interests. For more see *16.17 Loss of control of personal data* being processed due to installing of mobile app through third-party app store
.

8.4 Data subjects

The teachers, non-salaried staff and other data subjects whose personal data are being processed in HR2day have an interest in the careful and (GDPR-)compliant handling of their data. They also have an interest in their employer having a well-functioning HR-system, which enables them to access the data they need to do their job and exercise their HR- and payroll-related rights.

9 Processing locations and data transfers

9.1 Salesforce

The HR2day application and its databases are stored on Salesforce's Hyperforce infrastructure, which is hosted on AWS infrastructure.[61] HR2day has chosen Salesforce's data centres in Paris and Frankfurt to host the customer data that is processed when using HR2day. However, non-customer data, such as Salesforce controller data could leave the country of the chosen data centres.[62] The institutions' processor agreements with HR2day include descriptions of possible data transfers as a result of HR2day using Salesforce's services and state that the personal data processing takes place in the countries where the data centres are located.

In the following paragraphs, the possible data transfers that occur as a result of the use of Salesforce's services are described. According to the EDPB, a transfer is:

1) "A controller or a processor ("exporter") is subject to the GDPR for the given processing.
2) The exporter discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("importer").
3) The importer is in a third country, irrespective of whether or not this importer is subject to the GDPR for the given processing in accordance with Article 3, or is an international organisation."[63]

HR2day is subject to the GDPR for the processing of personal data in HR2day and qualifies as an exporter when disclosing these personal data to Salesforce. Since HR2day has a contract with Salesforce Inc., which is established in the USA, Salesforce qualifies as an importer in a third country if HR2day discloses personal data.

9.1.1 Law enforcement requests

The customer data, including personal data, as well as the backups are hosted in Salesforce's data centres within the EEA. This data is encrypted at rest and in transit using. The encryption keys are managed by Salesforce. When the personal data is stored in EEA data centres, with no reasonable way for USA authorities to access them, the mere risk of access from foreign authorities does not constitute a transfer.[64] When Salesforce does get a legally binding request to access personal data from a Public Authority, it has listed the steps it will take to notify the customer and resist the order.[65] Salesforce also guarantees that it will not provide any public authority with encryption keys and that it doesn't build

[61] https://help.salesforce.com/s/articleView?id=000396845&type=1, 20 May 2025

[62] https://help.salesforce.com/s/articleView?id=000795008&type=1, 20 May 2025

[63] *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, EDPB, p. 7

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

[65] Article 8.1 of the Salesforce DPA.

back doors into their products.[66] However, Salesforce has disclosed content and non-content data to public authorities before and has not guaranteed that it has never disclosed personal data from EU customers in the education sector. According to the transparancy report, which only includes requests that pertain to customer data, Salesforce has disclosed data in 86% of cases in response to 136 requests. The DPA also does not contain a 'canary clause' guaranteeing Salesforce will inform their customer (HR2day) when it's not able to comply with (a specific clause in) the DPA anymore, like challenging a law enforcement request, without having to state the reason for not being able to comply.

9.1.2 Customer support and technical operations support

By default, support is provided by staff within the EU and Salesforce does not have access to institutions' HR2day environment, unless the institution gives permission. However, when HR2day gives Salesforce permission to provide 24/7 support in high priority cases, institutions can provide access to customer data to support staff from outside the EU if the institution gives permission for this, for a set period of time. This DPIA assumes that the possibility of data transfers for support is covered in the processing agreement between HR2day and institutions, based on the sample of inspected processing agreements.

When HR2day provides personal data to support staff from Salesforce or from one of their sub-processors, by giving them access to these data through support requests, this constitutes a transfer. Salesforce can also give staff from their sub-processors access to these data. These sub-processors are located in:

- United States (adequacy decision)
- Argentina (adequacy decision)
- Australia
- Austria
- Brazil (adequacy decision)
- Canada (adequacy decision)
- France
- Germany
- India
- Ireland
- Israel (adequacy decision)
- Italy
- Japan (adequacy decision)
- The Netherlands
- Singapore
- South Korea
- Spain
- Sweden
- Switzerland
- Thailand

[66] Salesforce Transparancy Report, 14 March 2025, https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/2024-transparency-report.pdf, accessed on 17 October 2025.

- United Kingdom (adequacy decision)[67]

9.1.3 Technical operations support

To respond to technical or service problems, a team of Salesforce database administrators may, on occasion, require remote access to the database tables on which customers' personal data is hosted following "strict access and monitoring controls".[68] The sub-processors Salesforce may use for this are located in the same locations as the list in 9.1.2. Salesforce mentions the following purposes for this:

- Management of servers, connections and networks
- Providing technical and networking service
- Maintaining operations
- Troubleshooting hardware issues
- Quality assurance testing

These purposes are also covered in the processing agreement between HR2day and institutions.

According to the DPA between HR2day and the institutions, the following measures are in place to protect personal data.

- Use of software which blocks copying/pasting and printing of data
- Approval from senior management
- Documentation of access requests and logging of access
- Quarterly review of access
- Blocking of access upon termination of employment
- Multiple authentication levels

Additionally, data storage in Salesforce is such that the data has no value without the application logic.

- First and last names are not stored together, and the same applies to identifying codes
  such as national insurance numbers. Someone who has access to the database therefore does not know what data they are looking at
- The data and the application logic are stored separately. This is a fundamental part of the overall architecture of the Salesforce platform. The consequence is that unauthorised access to the database does not provide access to usable data.

SURF hasn't been able to verify these measures, but they are part of the contractual agreements between HR2day and institutions in SURF's sample.

---

[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, accessed on 15 October 2025.

[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, accessed on 28 January 2026, p. 7.

9.1.4 User Information Replication

Salesforce explains: “When Users log in to the Customer’s Salesforce environment, login requests will be sent to the nearest data center for authentication. The authentication process redirects the User to the appropriate data center for the duration of the active session. Salesforce may temporarily store identifying information about Users across its data storage locations outside of Europe for the purpose of facilitating the login process, even if all personal data is stored within Europe.”[69] When the MyDomain feature is enabled, the ability for users to login via *https://login.salesforce.com* and *https://welcome.salesforce.com* can be disabled, which prevents identifying data to be stored through the login process outside of Europe since users are forced to use their 'own' custom URL (hr2day-xxxx.salesforce.com).

SURF did not receive evidence that these settings were disbles in MyDomain.

9.1.5 Content Delivery Networks (CDN)

Salesforce states:

> *“Content delivery networks (“CDNs”) are utilized to optimize content delivery for certain Salesforce Services as listed in the Salesforce Infrastructure & Sub-processor Documentation. CDNs are commonly used systems of distributed services that expedite the transmission of content. Typically, a CDN is used to securely cache copies of content globally to better support end-users of the applicable Salesforce Services. Salesforce makes available the use of certain CDNs in conjunction with the Salesforce Services.”*[70]

The Salesforce Infrastructure & Sub-processor Documentation states that Salesforce uses global CDNs, using subprocessors Akamai Technologies, Inc., Amazon Web Services, Inc. and Cloudflare. They may process data in any country, regardless of the customer’s location and they route publicly cacheable content, static resources (like HTML pages, javascript and CSS files, images, and font files) and other cacheable webpage content.[71] It is unclear if the cached content includes personal data submitted by institutions. According to Salesforce, all communications between their CDN partner and Salesforce are conducted over HTTPs.[72] HR2day uses the standard caching setting, which means the data are cached for a minimum of five minutes and a maximum of ten minutes.

---

[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, accessed on 28 January 2026, p. 7, 8.

[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, accessed on 28 January 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, accessed on 28 January 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, accessed on 28 January 2026.

9.2 Possible additional transfers

During the technical investigation, end points belonging to third parties were found which are located in countries outside the EEA. Some of these can be attributed to the transfers described above and some of them result from processing of Google, Expo and SignRequest. It is unclear whether personal data is being transferred to the organisations responsible for these end points or if these organisations do any transfers themselves. In the processor agreements, no processing outside of the EEA has been recorded other than the transfers to Salesforce.

9.3 Transfer mechanisms

Currently, an adequacy decision from the European Commission – the Data Privacy Framework – applies to transfers between the EEA and the USA. Salesforce is covered by the DPF, so the transfers of personal data to Salesforce as a subprocessor have an adequate level of protection. However, since the dismissal of the chairman and two other members of the US Privacy and Civil Liberties Oversight Board (PCLOB), which is a core pillar of the DPF, the adequacy decision is under stress.

Salesforce also has binding corporate rules for processors (BCR-P) in place.[73] Binding corporate rules are essentially a set of data protection policies that all companies within a group adhere to, which has been approved by the relevant DPA and by the EDPB. These BCR-P apply to international transfers of personal data to and between members of the Salesforce Group, which includes all sub-processors of Salesforce.

Finally, the standard contractual clauses (SCC's) from the European Commission are part of the contractual framework between institutions and HR2day, so they apply to all transfers HR2day does. Right now, HR2day doesn't need to rely on these to guarantee an adequate level of protection. If the DPF is withdrawn, HR2day needs to carry out a DTIA on their transfers.

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

10 Retention periods and deletion

10.1 HR2day as processor

Institutions are responsible for determining and enforcing the retention periods for the personal data they are controller for.

In HR2day, users with the required level of access can delete data(sets). They can set general and specific expiry dates for documents. The current way of deleting data is through '*signal lists*'. These lists are generated periodically, i.e. every quarter, and contain all data (users, datasets, parts of datasets) that is supposed to be deleted. Through these lists these data sets can be deleted manually by a user with the 'extra rechten' profile. This profile only allows for deleting these documents, not accessing these documents.

HR2day has gotten in contact with her customers on how to better support, automate and enforce retention periods. For now, the outcome of these talks has led to the conclusion that the current way of working is still what the institutions/customers need. The main reasoning behind this is:

- It is an easily readable therefore accessible report
- Institutions/customers are reluctant towards automatic deletion. They prefer a human in the loop.

HR2day is able to develop automation in this process but are not instructed by their customers to do so.

For more see *16.14 Loss of control of retention periods because of lack of automation*.

10.1.1.1 Salesforce customer data

Article 9 of the Salesforce DPA refers to the following information:

> *"After termination of all subscriptions associated with any of the Covered Services "Subscription Termination"), Customer Data submitted to the Covered Services may remain in inactive status for up to 120 days. After such period, Customer Data will be overwritten or deleted from production within 90 days. Customer Data will be deleted from backups within 300 days of Subscription Termination. This process is subject to applicable legal requirements.*
>
> *Without limiting the ability for customers to request return of their Customer Data submitted to the applicable Covered Services, Salesforce reserves the right to reduce the number of days it retains such data after termination of the Covered Service. Salesforce will update this Security, Privacy, and Architecture Documentation in the event of such a change."*[74]

10.1.1.2 Logging

For retention periods on logging, please see *4.3.10 Logging*.

[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, accessed on 17 October 2025.

10.1.1.3 Backup
For retention periods on backups, please see ***Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.***.

10.2 HR2day as controller
In their privacy statement, HR2day states that it doesn't retain personal data longer than necessary for their purposes.

10.3 Salesforce
As explained in *4.3.10.1* Salesforce is collecting data[75], possibly personal data for their own purposes as one of the architectural principles.

SURF has received no further documentation on these logging practices by Salesforce and therefore cannot evaluate whether the retention periods are warranted.

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

Part B Assessment of Lawfulness of Data Processing

The second part of the DPIA assesses the lawfulness of the data processing. This part contains a discussion of the legal grounds, an assessment of the necessity and proportionality of the processing, and of the compatibility of the processing in relation to the purposes.

11 Legal Grounds

To be permissible under the GDPR, a controller must base the processing of personal data on one of the grounds mentioned in article 6(1) GDPR. These grounds are:

a. the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
b. processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c. processing is necessary for **compliance with a legal obligation** to which the controller is subject;
d. processing is necessary in order to protect the **vital interests** of the data subject or of another natural person;
e. processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller;
f. processing is necessary for the purposes of the **legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child

The assessment of available legal grounds (sometimes called 'lawful bases') is tied closely to the principle of purpose limitation. The EDPB notes that

> *"The identification of the appropriate lawful basis is tied to principles of fairness and purpose limitation. [...] When controllers set out to identify the appropriate legal basis in line with the fairness principle, this will be difficult to achieve if they have not first clearly identified the purposes of processing, or if processing personal data goes beyond what is necessary for the specified purposes."*[76]

Thus, in order to determine whether a legal ground is available for a specific processing operation, it is necessary to determine for what purpose(s), the data was or is collected and will be (further) processed. There must be a legal ground for each of these purposes. The appropriate legal ground furthermore depends on the role of the institutions and HR2day as controller or processor.

11.1 Legal grounds institutions

Institutions are controllers for all the customer data being processed in the HR2day processes described in chapter 4, except for 4.3.10.1 Salesforce. Below, some possible legal grounds for the institutions and some accompanying key points to consider when applying the legal ground will be discussed. Each institution has to determine their own legal grounds based on their specific processing.

[76] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects - version adopted after public consultation, 16 October 2019, URL: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en .

Legal ground e: public interest
Institutions have a legal obligation to perform a public task, namely the organisation of education. To invoke this basis, institutions must conduct a necessity test to demonstrate that the processing is necessary for the proper performance of their public task. For the processing of data that is not necessary for their public task, institutions may be able to apply one of the following bases.

Legal ground a: consent
Institutions mostly carry out the processing of HR and payroll data in the role of employer. As such, there is power imbalance between them and the data subjects, which means data subjects can't freely consent to the data processing. Therefore, institutions should generally refrain from using this legal ground for the processing in HR2day.

Legal ground b: performance of a contract
The processing in HR2day will likely be necessary for the performance of employment contract and contracts of services with the employees and non-salaried staff. Here too, institutions must carry out a necessity test to demonstrate that the purpose of the contract cannot be achieved without the relevant processing of personal data.

Legal ground f: legitimate interest
Processing that is not necessary for the performance of a contract may be necessary for the purposes of the legitimate interests pursued by the institution. In order to use this basis, institutions must assess whether institutions (1) have a legitimate interest, (2) the processing is necessary to represent this interest and (3) whether the interests of the institution outweigh those of the data subjects.

11.2 Legal grounds HR2day

HR2day describes the personal data processing it carries out for its own purposes in its privacy statement. It is unclear if HR2day uses data that were originally collected for the institutions' purposes or if HR2day collects these data as an independent data controller, due to the reasons as described in 7.4.1 HR2day. In response to this DPIA, HR2day has stated that their privacy statement doesn't apply to the HR2day application, but to the processing activities they carry out as an independent data controller. However, the privacy statement itself doesn't demonstrate this clearly. When HR2day is an independent controller, it depends on its own legal grounds, as (at least partially) described in the privacy statement.

For any further processing HR2day carries out with institutions' data for different purposes than the agreed purposes (mainly personnel administration, see 2 Purposes), HR2day determines the means and purposes and qualifies as a controller.[77] Institutions need to assess whether processing for these purposes is compatible with the purpose for which the personal data were initially collected.[78] If this is the case, the institutions also need to agree to the further processing in the processor agreements they conclude with HR2day. This assessment needs to take the following criteria into account:

[77] Article 28(10) GDPR.

[78] Article 6(4) GDPR.

a. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
b. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
c. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
d. the possible consequences of the intended further processing for data subjects;
e. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

11.2.1 User satisfaction

There is no direct link between the purpose of personnel administration and service improvement through collecting user satisfaction ratings, although service improvement could benefit a better personnel administration in HR2day. (a) HR2day doesn't have a direct contractual relationship with HR2day users, so they don't have a reason to expect HR2day will process their data for their own service improvement, apart from what's necessary to service the institution the user belongs to (b). The personal data collected has a low likelihood of containing special or sensitive data. However, this can't be ruled out due to the open text field available to leave comments. (c) The consequences for data subjects can be loss of
control and loss of confidentiality. (d) SURF has not been able to verify the existence or effectiveness of HR2day's safeguards in this process. (e) Therefore, HR2day's processing of user satisfaction data for service improvement leads to an incompatible further processing of personal data for HR2day's own service improvement purposes. Institutions have no way of disabling this functionality.

11.3 Legal grounds Salesforce

Salesforce is very clear about being processor for the customer data that falls under the DPA. However, Salesforce also has an extensive privacy statement about the processing of – amongst other things – the processing of users' usage data and logging data, which is also mentioned in their Hyperforce Security, Privacy and Architecture document. As described in 4.3.10.1 Salesforce, the documentation research and the testing haven't been able to show which data this concerns exactly and if these data were originally collected for the institutions' purposes. However, since Salesforce is only able to process these data due to the fact that institutions (indirectly) use its services for their own purposes, it is likely that at least some further processing takes place. As described in 7.4.2 Salesforce, Salesforce's own purposes include service improvement, security, and developing and deploying AI systems.[79] If Salesforce processes HR2day users' personal data for these purposes, institutions have to carry out the further processing assessment as described in 11.2.

Salesforce's privacy statement shows that they process personal data of end users of their services. As of this moment, SURF is not able to legally or technically rule out that this (further) processing takes place for HR2day end users. Institutions are unable to carry out a further processing assessment without knowing if and what personal data Salesforce

[79] The full list of purposes is available in the privacy statement (https://www.salesforce.com/company/legal/privacy/#privacy-statement, accessed on 29 January 2026).

processes for their own purposes, which means there can be no demonstrable legal basis for any further processing Salesforce does.

12 Special categories of data and sensitive data

12.1 Special categories of data

HR2day contains multiple types of special categories data, since it is an HR and payroll administration tool.

The biggest group is health data. HR2day can be used to register absences due to sickness and add information about the absence. Institutions are able to define their own classifications for absences. These classifications shouldn't contain more information about a data subject's health than is necessary for the employer's administration. Employers can use the existing guidelines for this.[80] It's also possible to add notes about an employee's absence in a free text field with the record. Furthermore, there are many classifications employers can add to employees with HR2day's built-in information about legal regulations, tax regulations and collective labour agreements. These classifications can also contain information about employees' health, for example when they show an employee has a right to (tax) benefits due to a disability or when they show the employers withholds sick pay.

The salary data about an employee can also be political data, when it shows the employee has been granted political leave, and data about trade union membership, when it shows the employer helps pay for trade union dues.

The nationality in combination with the place and country of birth shows a data subject's racial or ethnic origin, and can only be processed in this way if it is necessary to identify an employee or to use positive discrimination.[81]

HR2day has more open text fields which have the potential to be filled with special categories of personal data. By default, HR2day offers a maximum of ten open text fields with a specific purpose. These fields include an information icon which institutions can use to explain what type of data the field should contain. Additionally, open text fields can be added to any type of workflow. For example, a manager could record information about an employee's health in their performance review notes.

Since there are special categories of data being processed in HR2day, the institutions need to be able to rely on an exception to the prohibition of article 9 to be able to process these data. A likely exception for at least part of the health data is article 9(2)(b) GDPR, when "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law". This has been implemented in article 30(1)(b) of the Dutch implementation act of the GDPR, which allows health data to be processed by employers is the processing is necessary for:

[80] Beleidsregels verwerking persoonsgegevens gezondheid zieke werknemers, https://wetten.overheid.nl/BWBR0037896/2016-04-29, accessed on 29 January 2026.

[81] Autoriteit Persoonsgegevens, Personeelsdossier, https://www.autoriteitpersoonsgegevens.nl/themas/werk-en-uitkering/personeelsgegevens/personeelsdossier, accessed on 29 January 2025.

a. A proper implementation of statutory provisions, pension schemes or collective labour agreements that provide for entitlements dependent on the state of health of the person concerned; or
b. The reintegration or guidance of employees or benefit recipients in connection with illness or incapacity for work.

The Dutch DPA has published guidelines on what is and isn't necessary in 'De zieke werknemer'[82], the validity of which has been re-affirmed in its fine to CP&A[83].

12.2 Sensitive data

The main category of sensitive data is the financial data contained in the payroll administration. This data shows information about data subjects' financial situations. HR2day contains data about (changes to) data subjects' salary, additional (travel) compensations, pension, whether their wages are being garnished and all the components – legal and in their contract – that that make up their wages each period. There are also many free text fields which have the potential to inadvertently be filled with sensitive data.

The GDPR doesn't have additional rules for this type of data, but controllers need to take the increased risk of processing sensitive data into account when deciding on the appropriate technical and organisational measures necessary to comply with the GDPR.[84]

12.3 National identification numbers

Employers can process national identification numbers (bsn's) of employees and non-salaried personnel in HR2day.

Numbers used to identify a person that are prescribed by law may only be processed for purposes specified by law. The use of these numbers must be carried out with the utmost care and the necessity of using these numbers must be well substantiated[85]. In addition, Dutch law requires that the bsn may only be used by government bodies or by other organisations insofar as this is prescribed by law.[86] Employers and clients can only process the bsn for tax purposes under strict conditions.[87]

[82] Autoriteit Persoonsgegevens, De zieke werknemers, https://www.autoriteitpersoonsgegevens.nl/uploads/imported/beleidsregels_de_zieke_werknemer.pdf, accessed 15 October 2025.

[83] Autoriteit Persoonsgegevens, Boete CP&A verzuimregistratie, https://autoriteitpersoonsgegevens.nl/uploads/imported/boete_cpa_verzuimregistratie.pdf, accessed 15 October 2025.

[84] Article 24 GDPR.

[85] Article 87 GDPR and Article 46(1) of the Dutch implementation act of the GDPR.

[86] Article 1(d) of the General Provisions on Citizen Service Numbers Act (Wabb).

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

13 Purpose limitation

The principle of purpose limitation is that data may only be "collected for specified, explicit and
legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes".[88] Essentially, this means that the
controller must have a specified purpose for which it collects personal data, and can only process these data for purposes compatible with that original purpose. Data controllers must be able to prove, based on Article 5(2) of the GDPR, that they comply with this principle (accountability).

It is up to the institutions as controllers to decide for which purposes they process the data in HR2day. Chapter 2 shows an overview of likely purposes for the processing in HR2day. As data processors, HR2day and Salesforce are only allowed to process personal data for the purposes institutions determine in the processor agreements. If there is any personal data HR2day and Salesforce collect and process for their own purposes as independent data controllers, they must show which data these are and what the purposes are. If they carry out any further processing, they must provide institutions with the necessary information so they can show the processing is compatible with the original purposes the data were collected for by the institutions. 2 Purposes and 7.4 Other controllers have described the other purposes HR2day and Salesforce may process data subjects' personal data for. This DPIA has not been able to demonstrate that – contrary to what Salesforce's privacy statement shows – Salesforce doesn't process personal (usage) data from end users for their own purposes. HR2day's privacy statement also doesn't provide full clarity on whether HR2day further processes personal data for their own purposes and if yes, which ones, except for HR2day's processing of user satisfaction data for service improvement. The lack of transparency from both HR2day and Salesforce about the possible purposes they process personal data acquired through the application for means institutions cannot meet their accountability requirements.

[88] Article 5(1)(b) GDPR.

14 Necessity and proportionality

Each processing activity has to meet the necessity and proportionality requirements of the GDPR.

To prove a processing activity is necessary, a controller has to show that it is an effective way to achieve the intended purposes and that there is no less invasive way which in which the intended purpose can be achieved (subsidiarity).

To prove a processing activity is proportional, a controller has to show the invasion of privacy and the protection of the personal data of the data subjects is proportionate to the purposes of the processing. Proportionality demands a balancing act between the interests of the data subject and the data controller.

This chapter will examine if HR2day enables institutions to meet the necessity and proportionality requirements. Institutions can use this to perform a full assessment based on the details of their HRM and payroll processes.

14.1 Effectivity and subsidiarity

To assess the necessity of the processing activities in HR2day, the DPIA will examine if HR2day is an effective tool to achieve the purposes as described in chapter 2. There will also be an assessment whether there are less invasive alternatives (like other tools) available to HR2day to achieve the same purposes.

14.1.1 Effectivity

The institutions' main purpose is to be able to quickly and efficiently carry out HRM business operations "in the interests of a responsible personnel policy for both individuals and the organisation as a whole". Having a tool that combines human resources and payroll administration and helps automate and streamline processes is an effective way to achieve this.

14.1.2 Subsidiarity

To achieve the purpose of carrying out HRM business operations, most institutions will come to the conclusion that an HRM application like HR2day is necessary. Choosing which application to use has a big impact on the invasiveness of the personal data processing, since it determines which vendor institutions share their data with. The fact that Salesforce provides all of HR2day's architecture and hosting means that all personal data – customer data, usage data, logging data, etc. – gets shared with this big, US-based vendor who uses a lot of subprocessors. The possible further processing Salesforce does adds to the invasiveness of the processing through HR2day. The possibility of foreign law enforcement requests, due to Salesforce and its hosting parties being established in the US, also adds to the invasiveness. There may be other vendors of HRM applications who don't do any such further processing and don't host their data with US-based parties, making them less invasive in these respects than HR2day. This is something for institutions to take into account in their subsidiarity assessments.

Another point is that the HR2day+ mobile app is available via the Apple App Store and the Google Play Store. When a student downloads the app, a link is automatically created

between the use of the app and the student's personal Apple or Google account. This means having either an Apple account or a Google account is necessary to use the app, giving these platforms insight into the fact that the app has been installed and enabling them to combine this information with the other data they probably already have gathered about the user. This form of data processing is not strictly necessary for offering the app, as less privacy-invasive alternatives exist. For example, HR2day could choose to offer the app as a so-called 'sideload' outside the regular app stores, thereby minimising the involvement of Google and Apple, or enable opening HR2day in a browser.

The mobile HR2day+ app also sends push notifications. The push notifications cause both the
transfer of metadata and the content to Google and Apple. The metadata concerns data such as device identifiers, IP addresses and possibly the student's Google or Apple account. The content concerns the messages if that content is sent unencrypted, as is necessarily the case with the "notification messages" part of the push notifications. The content of these messages is visible to and processed by Google and Apple. Institutions determine the content of the messages themselves and can make privacy-friendly choices, for example by not including personal data. Regardless of the content of the messages, the use of notification messages means that the content of the messages is systematically processed by Google. It is possible to reduce this by using an encrypted data payload, whether or not on top of the notification message. If a student has Unified Push, an alternative push infrastructure for Android, available, the app can also use this and fall back on Google if it is not available.

14.2 Proportionality

To assess the proportionality of the processing activities, it must be weighed if the invasiveness of the activities is proportionate to the purposes of the activities. The assessment of the invasiveness has to take into account the (privacy) interests of the data subjects. To structure this weighing exercise, four of the principles from article 5 of the GDPR will be used.

14.2.1 Lawfulness, fairness and transparancy

Lawfulness means that all the legal conditions for data processing are adhered to. The institutions have their own legal grounds and HR2day does have processor agreements. However, for subprocessor SignRequest, there are also a lot of data transfers that seem to happen which aren't accounted for in the (sub)processor agreement. Furthermore, if HR2day and Salesforce do carry out further processing activities, institutions can't demonstrate they fulfil the requirements for compatible further processing based on article 6(4) GDPR. There also additional recipients that may need to be qualified as subprocessors, for which there are no subprocessor agreements available.

The principle of *transparency* not only ensures that consent must be informed but that full transparency of data practices and rights is ensured to users. Because of the lack of information about specifically Salesforce data processing practices with HR2day users' data, HR2day and institutions can't meet this requirement. There is also unclarity surrounding HR2day's privacy statement and processing for its own purposes. Finally, the lack of logging and monitoring on which information an administrator accessed while using the proxy login functionality causes a lack of transparancy.

Fairness is an overarching principle which requires that personal data shall not be processed in a way that is detrimental, discriminatory, unexpected, or misleading to the data subject.[89] Because of the lack of transparency, it can't be assessed if any further processing is fair to data subjects and aligns with their reasonable expectations of the (metadata about the) processing of their HRM and payroll data.

In conclusion, without being able to rule out that HR2day and Salesforce further process personal data for any purposes not in line with the institutions' purposes, they can't use HR2day in a way that aligns with the lawfulness, fairness and transparancy principle. There should also be logging of the information that was accessed using the proxy login functionality.

14.2.2 Data minimisation

The principles of data minimisation and privacy by design require that the processing of personal
data be limited to what is necessary. The data must be 'adequate, relevant and limited to what is
necessary for the purposes for which they are processed' (Article 5(1)(c) of the GDPR). This means that the controller may not collect and store data that are not directly related to a legitimate purpose. According to this principle, the default settings for the data collection should be set in such a way as to minimise the data collection by using the most privacy friendly settings.

HR2day offers many possibilities to design workflows for different processes with different types of fields within its data model, among which open text fields. It is up to the institutions to ensure they only process the data necessary for their processes and use open text fields in such a way that it is clear what their purpose is, so they don't invite users to share more personal data than necessary.

Salesforce sets a lot of cookies on HR2day and the purposes for some of these are described in a way that makes it hard to assess if the data they collect is necessary for legitimate purposes. This causes possible infringement on the data minimisation principle. Furthermore, the fact that SURF hasn't received an exhaustive list of the data fields Salesforce collects, means that it can't be assessed if the data minimisation principle is adhered to. There is also a lack of information about Salesforce's anonymisation practices, specifically for their logs, so it can't be assessed if this is done properly with respect to the data minimisation principle.

Lastly, it's not possible to restrict access only to the personal data users need to be able to fulfil their tasks when the vertical rights inheritance functionality is turned on. This means persons higher up in the hierarchy have access to more personal data than necessary. This functionality is turned on by default, and organisations that assign HR functionalities to managers 'in the line' need to turn it on for HR2day to function as required.

[89] EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and Default, version 2.0, adopted on 20 October 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, accessed on 17 October 2025.

In conclusion, institutions can control mostly their data minimisation practices with regard to the personal data they choose to record in HR2day. However, it can't be assessed if the data minimisation principle is adhered to with regard to Salesforce's processing of usage data, due to a lack of information. The vertical rights inheritance functionality also causes a data minimisation dilemma for institutions.

14.2.3 Accuracy

The principle of accuracy requires that the personal data be accurate and, where necessary, kept up to date. "[E]very reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay" (article 5 (1) (d) GDPR).

HR2day offers connections to automatically import data from (recruitment) systems, ensuring data accuracy when entering data into the application. If data in the application is nevertheless incorrect, HR2day offers functionalities to correct it.

In conclusion, no technical or functional limitations have been found within HR2day that prevent educational institutions from complying with the principle of accuracy.

14.2.4 Storage limitation

The principle of storage limitation demands that personal data are only retained as long as necessary for the purpose in question. Data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" (article 5 (1) (e), first sentence GDPR). This principle therefore demands that personal data are deleted as soon as they are no longer necessary to achieve the purpose pursued by the controller.

HR2day offers the institutions the possibility to enforce their own retention periods for customer data through signal lists and through the functionality of putting automatic retention periods on documents.

The retention periods determined by HR2day as described in 4.3.10 Logging and 5.8 Back-up are in line with industry standards.

Salesforce retain the data it processes for HR2day as a processor for as long as the subscription to the Salesforce services is active and HR2day or the institutions do not delete the data themselves. After termination of the subscription, Salesforce retains the data for 120 days in inactive status. After this, the customer data is overwritten or deleted from production within 90 days. The data is deleted from backups within 300 days after termination of the subscription. While these are fairly standard industry periods, HR2day needs to offer institutions the possibility to delete these data at an earlier time.

For any possible further processing Salesforce carries out, it is unclear which retention periods they handle and if these adhere to the principle of storage limitation.

In conclusion, institutions are able to adhere to the storage limitation principle for data that is under their and HR2day's control. However, it can't be assessed if this is also the case for processing by Salesforce.

14.2.5 Integrity and confidentiality

Personal data must be processed in such a way that appropriate security is guaranteed and that it is protected against, among other things, unauthorised or unlawful processing and against accidental loss, destruction or damage (Article 5(1)(f) GDPR in conjunction with Article 32(1) and (2) GDPR).

Read access logging

The absence of logging for data access (read access logging) increases the risk that it cannot be determined whether unauthorised individuals have viewed personal data in cases of an authorization error or incident. As a result, in the event of a potential data breach, it is impossible to ascertain whether, and whose, personal data has been viewed by unauthorised users. This means institutions cannot take adequate and targeted measures.[90]

Authorisation

HR2day offers detailed authorisation features as described in 4.3.9 Managing roles and profiles. However, the use of the vertical inheritance of rights causes a situation where persons high up the hierarchy have very broad authorisations enabling to access all personal data of all employees in the vertical line below them in the hierarchy, which may surpass their actual needs. The result of turning this functionality off is that the supporting processes/workflows can't be followed at the various management levels, which is necessary when HR duties are assigned to managers 'in the line'. It's also not possible to restrict access only to the personal data users need to be able to fulfil their tasks, causing a breach of confidentiality and data minimisation when this functionality is turned on at organisations who assign HR duties to managers in the line.

Encryption

For encryption, HR2day relies on Salesforce's encryption practices. Data is encrypted at rest and in transit according to industry standards. However, the management of the encryption keys lies with Salesforce, which means HR2day can't control who accesses their encrypted information in practice.

Special and sensitive categories of data

Since processing of sensitive and special categories of data inherently have a higher risk level, there need to be additional security measures to ensure an appropriate level of security. Salesforce offers additional encryption options through its Salesforce Shield service, which is specifically designed to add extra protection for sensitive data and special categories of personal data.[91] However, HR2Day does not use these enhanced encryption

[90] It is a sector standard to implement read access logging on personal data in ERP and HRM systems. See: Richtlijn Logging en Monitoring, https://sec.surf.nl/asset/template-richtlijn-logging-en-monitoring/?category=richtlijnen, p. 16, accessed on 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, accessed on 17 October 2025.

levels. As a result, sensitive and special category data are not additionally protected with cell-level encryption.

In conclusion, the absence of read access logging, the settings of the vertical inheritance of rights and the lack of additional encryption options for sensitive and special categories of data restrict institutions in creating integrity and confidentiality in their HR2day environment.

15 Data subject rights

The GDPR grants data subjects the right to information, access, rectification and erasure, object to profiling, data portability and file a complaint. It is the data controller's obligation to provide information and to duly and timely address these requests. If the data controller has engaged a Data Processor, the GDPR requires the DPA to include that the Data Processor will assist the data controller in complying with data subject rights requests. This chapter assesses whether institutions and HR2day meet the GDPR requirements relating to data subjects' rights and whether data subjects can effectively exercise such rights.

15.1 Right to information

Data subjects have a right to information (Articles 12-14 GDPR). This means that data controllers must provide them with easily accessible, comprehensible and concise information in clear language about, inter alia, their identity as data controller, the purposes of the data Processing, the intended duration of the storage and the rights of data subjects.

There is a lack of information in HR2day's privacy statement about whether it applies to the HR2day application and if yes, which parts. While HR2day did end up providing all information about its cookies, there is currently no complete cookie statement for users. The role of Salesforce and the personal data it processes are also not clearly communicated.

15.2 Right to access

Data subjects have a fundamental right to access personal data concerning them (article 15 GDPR). Upon request, data controllers must inform data subjects whether they are processing personal data about them (directly, or through a Data Processor). If this is the case, they must provide data subjects with a copy of the personal data processed, together with information about the purposes of processing, recipients to whom the data have been transmitted, the retention period(s), and information on their further rights as data subjects, such as filing a complaint with the Data Protection Authority.

As data controllers, institutions must comply with Access Requests filed by data subjects. HR2day must assist institutions in doing so.

The response to the DSAR request to HR2day was incomplete (see 1.2 Data Subject Access Request for the full response). HR2day did provide the in-application data about the data subjects, the login history and the mutation logs. However, any further logging that HR2day carries out according to the documentation they provided was missing. Additionally, there has been no information provided about any (further) processing Salesforce and HR2day do, like processing data about the usage of the HR2day service. The personal data processed through subprocessor Expo and SignRequest was also missing.

15.3 Right to object

Data subjects have the right to object to processing based on legitimate interests or public tasks, as well as direct marketing (article 21 GDPR).

Insofar institutions perform any processing activities based on their legitimate interest(s), they must facilitate the right to object. HR2day is obliged to assist institutions, insofar reasonably possible, in facilitating such objections.

15.4 Right to rectification and erasure

Data subjects have the right to have incorrect or outdated information corrected, to have incomplete information completed (Article 16 GDPR), and under certain circumstances to have personal data deleted (Article 17 GDPR).

HR2day offers the possibility to easily correct and delete data in the application. If incorrect or incomplete personal data is processed in log files, this is due to an incorrectness or incompleteness in the source data, i.e. the personal data registered at account creation. By their very nature, log files record the personal data as it is recorded in the source data. Therefore, any request to rectify this data should be aimed at the source data, rather than the data in log files. Regarding erasure requests aimed at personal data in log files will usually not be applicable as none of the grounds in Article 17(1) GDPR apply. The purpose of processing this personal data is to ensure the security of personal data, and the HR2day environment more broadly. The personal data recorded in log files will remain necessary for this purpose until these log files are deleted in line with the applicable retention policies. Moreover, rectifying or erasing personal data from log files would undermine this purpose and could compromise the protection of data subject's personal data required by the GDPR.

Part C Description of risks

This part concerns the description and assessment of the risks for data subjects. These are the risks as found during testing and analysis and before taking mitigating measures. The risks will subsequently be classified according to the likelihood they might occur, and the impact on the rights and freedoms of the data subjects when they do. The model this DPIA, based on “het Rijksmodel”, uses the risk categories and the risk model of the British Data Protection Authority, ICO. ICO lists the following main categories of risks:

- inability to exercise rights (including but not limited to privacy rights);
- inability to access services or opportunities;
- loss of control over the use of personal data;
- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage.

These main categories give guidance to determining specific risks. By representing the risks encountered according to their potential impact on the rights and freedoms of data subjects, a picture of the high and low risks emerges. This is displayed in the risk graph developed by the UK regulator ICO, as follows:

Table: ICO Risk model

Severity of impact	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood/Probability of harm		

This DPIA uses the following meanings of the “likelihood of harm” and the “severity of impact” to assess the risks:

Likelihood	**Meaning**
Very small	It is unlikely that this risk will occur
Reasonable possibility	It is conceivable that this risk will occur.
More likely than not	It is likely or certain that the risk will occur

Impact	Meaning
Minimal impact	The consequences for the data subject have little or negligible impact on the data subject's rights and freedoms when the risk occurs
Some impact	The consequences for the data subject have a limited impact on the rights and freedoms of the data subject upon the occurrence of the risk
Serious harm (severe impact)	The consequences for the data subject have a substantial impact on the rights and freedoms of the data subject upon the occurrence of the risk

16 Risks

Salesforce risks

16.1 Loss of control and loss of confidentiality due to unauthorised access through transfers to Salesforce

HR2day ensures that Salesforce hosts their customer data in data centres within the EEA. The transfers that occur due to having Salesforce as a processor are described in the paragraphs about, User Information Replication and Content Delivery Networks (CDN).

Salesforce is a US based company, meaning they fall within the scope of US law. Therefore, as described in 9.1.1 Law enforcement requests, there is a chance that Salesforce is legally compelled to disclose personal data to US authorities based on US law such as the CLOUD act. Since Salesforce handles the encryption key management, the data concerned could be decrypted personal data in customer data, logging data and IP addresses of data subjects, as well as any personal data in the Salesforce usage data. The DPA between Salesforce and HR2day requires Salesforce to inform HR2day about, and forward, third party orders to disclose personal data, challenge any such orders and indemnify data subjects in case personal data has been transferred – in so far legally permitted. However, it does not contain a canary clause that will require them to inform an institution of their inability to comply with their contractual obligations if they receive a request accompanied by a gag order.

Furthermore, Salesforce provides support services as described in 9.1.2 Customer support and technical operations support and 9.1.3 Technical operations support, which means personnel from five third countries could gain access to customer support data and database tables. There are organisational and technical measures in place to minimise this access and ensure that when access does happen, minimal negative consequences can happen.

Finally, as described in 9.1.4 User Information Replication and 9.1.5 Content Delivery Networks (CDN), login requests may be stored outside the EU (although HR2day states it doesn't use this functionality) and Salesforce uses a CDN.

Salesforce's transparency report shows that it has received and complied with requests for both content and non-content data before. However, the described existing measures for the data transfers in combination with the existence of the protections of the Data Privacy Framework (which also provides protection for onward transfers), Salesforce's BCR-P and the SCC's means that as long as the Data Privacy Framework exists, the probability of a negative impact for data subjects is very small. This does require all transfers to be properly recorded in the DPA between institutions and HR2day, so these legal protections apply to the transfers. When they aren't recorded, the probability of harm is more likely than not, since these protections don't apply. When there is unauthorised access or disclosure, it causes a loss of control for data subjects which may lead to serious harm to their rights and freedoms. For example, their (sensitive or special categories of) personal data could be processed for unknown purposes (like surveillance) with no opportunity for redress. As

such, this risk is currently low for institutions who have recorded the Salesforce data transfers, and high for institutions who haven't.

16.2 Loss of control due to a lack of transparency about processing usage data for purposes Salesforce

Salesforce's privacy statement states that Salesforce may process information about users' devices and their usage of Salesforce's services through log files and other technologies. This privacy statement applies to all Salesforce services, including HR2day's platform. It rules out Salesforce processing customer data for its own purposes, but since the DPA only includes customer data, this leaves the possibility of Salesforce processing types of data not included in the DPA, like logging data and usage data. Salesforce claims it processes usage data in a way that doesn't allow them to identify identification of individuals. SURF hasn't witnessed any processing of personal data by Salesforce as described in the privacy statement, because SURF isn't able to access Salesforce's processing, due to technical reasons amongst others. Therefore, SURF also hasn't been able to (technically) verify the absence of this processing or legally rule it out. So, it's unclear what personal data is collected by Salesforce, for what purposes, what the retention periods are and how Salesforce applies pseudonymisation and anonymisation techniques. HR2day hasn't been able to provide an exhaustive list of data fields Salesforce collects in their usage data, nor an explanation about their anonymisation techniques. SURF can't rule out that Salesforce doesn't process HR2day's users' personal data in the ways described in the privacy statement, including the subsequent processing for their own purposes, like service improvement. Since no compatibility test has been carried out and any further processing activities aren't included in the processor agreements, the possibility of this further processing results in a loss of control.

The probability of a loss of control happening is more likely than not, since – despite HR2day's best efforts of obtaining this information – Salesforce hasn't been able to provide sufficient reassurances to counteract the information in their privacy statement. This causes serious harm for the data subjects, because the data processing as described in Salesforce's privacy statement is extensive, the data concerned could be sensitive or special and institutions have no control over the processing of this data. Salesforce also includes processing purposes like training AI models in its privacy statement, which is a purpose that is far removed from the institutions original purposes in processing their HR and payroll data and not in line with data subjects' reasonable expectations. Additionally, the lack of transparancy means that institutions can't comply with the information rights of their data subjects. Therefore, this is a high risk.

16.3 Inability to exercise data subject access rights to personal data

The response to the DSAR request to HR2day was incomplete. HR2day did provide the in-application data about the data subjects, the login history and the mutation logs. However, any further logging that HR2day carries out according to the documentation they provided after they provided their DSAR response, namely the event monitoring, setup audit trail and email logs, was missing in the DSAR response. Additionally, there has been no information provided about the usage data Salesforce processes as subprocessor. The personal data processed through subprocessors Expo and SignRequest and possible subprocessors Google and Apple was also missing.

This creates the risk that data subjects are unable to effectively exercise their rights under the GDPR. The probability of this happening is more likely than not, since it did occur. Failure to meet the deadline for the DSAR, even for part of the data, results in serious harm to the rights of the data subject, since the right to access is a fundamental right. Therefore, this risk is high.

16.4 Loss of control due to lack of transparency about processing of personal data through cookies

HR2day doesn't have a cookie statement documenting the cookies HR2day and its subprocessors (most importantly Salesforce) use to collect personal data. Therefore, data subjects aren't able to inform themselves about the processing HR2day and their sub-processors perform through cookies before the processing begins and exercise their rights.

The probability of this happening is more likely than not, since there isn't a complete cookie statement at the moment. This causes serious harm to data subjects, since they can't exercise their data subject rights. Therefore, this is a high risk.

16.5 Loss of control due to having to register for subprocessor updates Salesforce

To get notified of new subprocessors of Salesforce, resellers and customers must register for updates through their form. Some HR2day employees are registered for these updates, but there is no known process for informing institutions about new subprocessors, so institutions are able to carry out their processor agreement rights. Institutions not being notified of new subprocessors would constitute a violation of their processor agreements.

There is a reasonable possibility of this occurring as there is no guarantee institutions are informed about new subprocessors. Without proper information, data subjects are not put in a position where they can effectively exercise their data subject rights, leading to a loss control causing serious harm. The overall risk is high.

General risks

16.6 Loss of control due to a lack of transparancy about processing personal data for purposes HR2day

HR2day's statement states that HR2day may collect and process data about users for their purposes, like improving their services. The wording of this statement doesn't make it clear if HR2day uses personal data it has obtained as a processor for this. This lack of clarity about HR2day's processing prevents institutions from properly informing their data subjects about their personal data processing and about any further processing that may take place.

The probability of a loss of control happening is more likely than not, since the current privacy statement leaves open the possibility of HR2day processing customer data for their own purposes. The further processing causes serious harm, since it is unclear which personal data this concerns and the data could be sensitive or special. A purpose like "Creating interest profiles for promoting relevant products and services (profiling)" is also

not in line with the institutions original purposes and data subjects' reasonable expectations. Therefore, this is a high risk.

16.7 Loss of control of user satisfaction data

HR2day collects user satisfaction data for service improvement purposes through pop-ups. Institutions aren't able to turn off this functionality, access these data or influence what HR2day collects. These reviews aren't part of the processing agreements with the institutions and institutions have no way to instruct HR2day about this processing. HR2day's processing of user satisfaction data for service improvement leads to an incompatible further processing of personal data for HR2day's own service improvement purposes.

The probability of this happening is more likely than not, as it is HR2day's current practice to do this. There is some impact to data subjects, since the fact they have no reason to expect HR2day will process their data for their own service improvement causes a loss of control. However, the concerned data set is limited. Therefore, this is a high risk.

16.8 Loss of control and loss of confidentiality by unauthorised access in third countries

During the technical research, transfers outside of the EEA were found in relation to subprocessor SignRequest for electronically signing agreements, subprocessor Expo for sending mobile app notifications and Google for using the Google Maps integration. The transferred data can be customer data, but also other data like logging data. The transfers were partly to the USA, to which the Data Privacy Framework applies, but it is unclear whether there were any more (onward) transfers.

Since these transfers aren't protected legally in the processor agreements and no other measures to protect the concerned personal data, the probability of a loss of control is more likely than not. This is especially the case for SignRequest, who have demonstrated that they can't enable institutions to process data in a way compliant with the GDPR. The impact on the rights and freedoms of data subjects if happens can be serious harm depending on the type of personal data that is disclosed and the party it is disclosed to. Therefore, this is a high risk

16.9 Loss of control of subprocessors and recipients through lack of or incorrect agreements

HR2day has a processor agreement with Expo, but hasn't provided the accompanying main service agreement to SURF. There is a service agreement and subprocessor agreement with SignRequest, but SignRequest also requires users to agree to their own privacy statement when HR2day users get redirected to their services. This creates a contradicting message about SignRequest's role. Furthermore, there are some recipients with which there are no agreements of any kind. These recipients are Google and Apple, who process data about data subjects when using the HR2day app and when using the Google Maps integration. They should either be subprocessors, which means HR2day should have subprocessor agreements with them, or third party recipients who are joint/independent controllers. In the latter case, institutions have to give permission for providing their personal data to these parties.

The lack of documentation causes a lack of transparency about the data being processed by their parties and a loss of control of these data. The probability of this happening is more likely than not, since the documentation is currently lacking. This can cause serious harm to data subjects, since the lack of agreements means there is no control at all over these data and data subjects aren't able to exercise their data subject rights. Therefore, this is a high risk.

16.10 Loss of confidentiality due to absence of 'read access logging'

The absence of logging for data access (read access logging) increases the risk that it cannot be determined whether unauthorised individuals have viewed personal data in cases of an authorisation error or incident. As a result, in the event of a potential data breach, it is impossible to ascertain whether, and whose, personal data has been viewed by unauthorised users. This means institutions cannot take adequate and targeted measures.

There is a reasonable possibility of these consequences occurring, because the absence of read access logging makes it difficult to monitor and mitigate unauthorised viewing. The result is serious harm, because special and/or sensitive personal data may be involved, and access by parties both inside and outside the organisation may take place. This is a high risk.

16.11 Breach of data minimisation by including too broad lists for reasons for absenteeism

Overly broad lists for reasons for absenteeism in HR2day represent a breach of the GDPR data minimisation principle. This principle mandates that personal data collected must be adequate, relevant, and limited to what is necessary for the specific purposes for which it is processed. The ability of institutions to define their own categories for illness or other absenteeism reasons leads to risks of excessive and unnecessary collection of sensitive data. This can result in the processing of health and other special category data beyond the minimum necessary, infringing on employees' privacy and increasing the chance of improper data use or breaches.

The probability of this risk manifesting is highly dependent on the maturity of the institutions' team configuring and administering HR2day, so it is more likely than not that it will occur. The impact can be serious harm due the nature of the purposes HR2day fulfils at institutions. Therefore, this is a high risk.

16.12 Loss of control through open text fields

The presence of potentially numerous open text fields in HR2day, while often properly labelled with intended purposes, poses a risk of loss of control over personal data. Not all methods of field validation are implemented, which can lead to inconsistent or inaccurate data entries. Institutions/customers can also create new text fields without attaching proper purposes or adequate labelling, exacerbating the risk of uncontrolled data collection and processing. From a privacy perspective, open text fields are particularly sensitive because users can input any type of personal or sensitive information, potentially exceeding the intended scope of data processing or violating data minimisation principles.

The likelihood of this occurring is more likely than not, since it is highly dependent on the maturity of the institutions' team configuring and administering HR2day. The impact can be

severe, depending on the type of data that is shared, which can be sensitive or special. Therefore, this is a high risk.

16.13 Lack of accuracy through manual registration of personal data

The possibility of manual registration and editing of personal data in HR2day poses a risk of data inaccuracy due to human error. Managers and HR staff can directly input and modify personal details such as employment relationships, salaries, leave records, and user information. The absence of automated validation or standard controls during manual data entry increases the likelihood of incorrect or outdated information being recorded. This can lead to unintended consequences such as sharing information with unauthorised parties, financial discrepancies, and employees being incorrectly denied leave. This situation underscores the importance of implementing corrective controls such as input validation, audit trails, and periodic data reviews to enhance data accuracy and reduce privacy risks. Ultimately, ensuring high data quality safeguards not only individuals' privacy but also the integrity and reliability of HR operations.

The probability of these inaccuracies occurring is considered more likely than not, as the risk is dependant on the maturity of the institutions' team configuring and administering HR2day combined with the lack of current mitigation measures. Without mechanisms for error detection or correction integrated into the system, errors may persist unnoticed and propagate through related processes. Since these errors directly affect individuals' rights and entitlements causing tangible and meaningful consequences, the impact for data subjects can be serious harm. Because of the serious impact and the reasonable likelihood, this is a high risk.

16.14 Loss of control of retention periods because of lack of automation

HR2day currently lacks automated functionality to delete personal data once retention periods expire, and it cannot generate alerts when such periods end. Distinctions between categories of personal data with different retention requirements are also not systematised. The current approach relies on periodic manual handling of signal lists, which are likely inconsistently managed with extended intervals between deletion actions. This creates a significant risk that personal data remains stored longer than necessary, violating data minimisation principles and leading to a loss of individual control and confidentiality.

The probability of this risk manifesting is more likely than not due to the dependency on manual processes vulnerable to human error and oversight. This can cause serious harm, as this issue affects the principle of storage limitation for all personal data managed in HR2day, including special categories of sensitive data. Therefore, this is a high risk.

16.15 Loss of confidentiality due to vertical inheritance of rights default setting

The default setting of vertical inheritance of rights within the system leads to a conflict with the data minimisation principle mandated by the GDPR. Vertical inheritance allows rights to be passed up through organisational layers automatically, which can result in broader access than necessary to personal data. While disabling this inheritance would enhance privacy protection by limiting access only to those authorised, it also creates, in some cases, operational challenges for organisations who assign HR duties to managers 'in the line'. This situation exposes a significant risk of loss of confidentiality, because excessive

inherited access rights may allow users to view or manage personal data beyond their legitimate scope. To align with the data minimisation principle, the system must enable granular access control that supports restricting groups' access appropriately while maintaining necessary functional workflows.

The likelihood of this risk manifesting is reasonable. Even though HR2day informs institutions about the option to turn it off, the vertical inheritance of rights setting is turned on by default. Institutions who assign HR duties to managers in the line have to enable vertical inheritance of rights for them to carry out their tasks and may not realise the impact of this, therefore not using the proper measures to prevent harm to data subjects. The impact is serious, because excessive inherited access rights may allow users to view or manage personal data, including sensitive and special categories of personal data beyond their legitimate scope. Therefore, this is a high risk.

16.16 Loss of control through lack of encryption key management

Salesforce as a sub-processor is responsible for hosting, encryption, backup, and additionally manages the encryption keys used in these processes. While the sub-processor must implement technical and organisational measures to ensure security, the ultimate responsibility for data protection compliance remains with the controller. HR2day's delegation of key management to a sub-processor adds an additional layer where key management failures can lead to unauthorised decryption and data breaches. Since HR2day itself is not in charge of key management or storing the keys, the controller must ensure through contractual and audit mechanisms that the sub-processor employs robust encryption key management practices including secure key storage, access restrictions, rotation policies, and incident monitoring. Without strict controls and transparency, reliance on a sub-processor for key management can weaken security posture and complicate breach notifications if keys are compromised. Having HR2day store and manage the encryption keys also ensures that no personal can be shared by Salesforce if they receive disclosure orders from foreign authorities.

To demonstrate how the data in the HR2day application is encrypted, HR2day referred to general Salesforce security certifications and other Salesforce documentation. This documentation describes, scattered over at least four different documents[92], the types of encryption Salesforce offers and offers assurances that customer data and back-ups are encrypted at rest. However, they don't offer detailed insight in how encryption is implemented for Salesforce services in general (encryption protocols, how often keys are rotated, where keys are stored, etc.), and especially not for HR2day specifically. The only known facts are that HR2day uses database encryption and doesn't use Salesforce Shield. HR2day contains sensitive and special categories of data, which demand enhanced protection measures beyond standard safeguards, because their disclosure can lead to significant harm. Salesforce itself recommends considering using additional Platform Encryption (offering cell-level encryption) for sensitive data. Cell-level encryption offers an additional level of protection once the main encryption keys are compromised.

[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.

The likelihood of a loss of control occurring once there is a breach of security is more likely than not, since HR2day depends fully on Salesforce for managing the encryption methods. The impact is serious as this issue affects all personal data managed in HR2day, including special categories of sensitive data, for which there are no additional measures in place by default. Therefore, this is a high risk.

Risks as a result of offering a mobile app through the Google and Apple app stores

At the time of publication, SURF hasn't reached a conclusion about the impact of the following two risks, which are associated with the processing by Google and Apple when using mobile apps. The considerations and measures SURF has identified are written down below. However, SURF is doing a further investigation into the impact of these risks and the effect of available measures on the risks. There will be a publication about this at a later time. In the meantime, institutions can take action based on their own assessments.

16.17 Loss of control of personal data being processed due to installing of mobile app through third-party app store

The risk associated with offering the HR2day mobile app through the Apple App Store and Google Play Store lies in the automatic linkage created between the app usage and the user's personal Apple or Google account. This linkage enables these platform providers to gain insights into the installation of the app, which can lead to indirect identification of the relation to HR2day. Because this processing is not strictly necessary for the app's functioning, it conflicts with the Privacy by Default principle a result in loss of control over personal data.

The likelihood of this risk materialising is more likely than not, since a loss of control will occur once the app is downloaded through an apps store. Consequently, personal data about employees inevitably flows to third parties like Apple and Google, potentially compromising confidentiality and increasing the risk to employees' rights and freedoms. This causes the potential exposure of personal data without explicit necessity and the involvement of large platform providers.

Alternatives with fewer privacy intrusions should be considered to better protect users' data and ensure compliance with data minimisation requirements.

16.18 Loss of control due to processing of push notifications by Google and Apple

This is a risk that applies generally to all applications that use the push infrastructure of Google or Apple.

The mobile HR2day app sends push notifications. The push notifications cause both the transfer of metadata and content to Google and Apple. The metadata concerns data such as device identifiers, IP addresses and possibly the student's Google or Apple account. The content concerns the messages if that content is sent unencrypted, as is necessarily the

case with the “notification messages” part of the push notifications. The content of these messages is visible to and processed by Google and Apple. Since it’s not necessary to include personal data in notifications, doing this constitutes a breach of the subsidiarity principle. Educational institutions determine the content of the messages themselves and can make privacy-friendly choices by not including personal data.

Regardless of the content of the messages, the use of notification messages means that the content of the messages is systematically processed by Google. It is possible to reduce this processing by using an encrypted data payload, either on top of the notification message or separately. If a student has Unified Push, an alternative push infrastructure for Android, available, the app can also use this and fall back on Google if it is not available. Given the absence of both mitigating measures, the use of notification messages does not comply with the subsidiarity requirement.

The probability of a loss of control occurring is more likely than not, since notifications are a standard part of the HR2day app and the loss of control occurs as soon as Google or Apple receives the notification.

Part D Description of proposed measures

Driving innovation together

17 Measures

This chapter describes the technical, organisational and legal measures that institutions and HR2day can take to mitigate the risks described above. For each risk, the upper half of the table describes the current risk and shows the risk score from section C. The lower half of the table describes the measures that HR2day and the institutions can take and gives a score for the residual risk.

This reference DPIA assumes an adequate baseline of organisational privacy maturity. However, the applicability and prioritisation of both risks and measures will vary significantly depending on each institution's current process, technical and governance maturity levels. We strongly advise any institution that questions its readiness to conduct a self-assessment against the presented risks and measures or seek guidance from peer institutions, SURF and/or MBO Digitaal. It is paramount that each institution critically evaluates this overview against its own operational context and technical infrastructure.

Salesforce risks

Loss of control and loss of confidentiality due to access to personal data by foreign authorities						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	**Current risk**
16.1	Access to personal data by foreign authorities	Loss of control and loss of confidentiality	**More likely than not**	**Serious**	**High**	
	Measures Institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	**Residual risk**
	-*	Include all lawful transfers in DPA between institutions and HR2day.	**Remote**	**Serious**	**Low**	

*While legally, no additional measures on the side of the institution are necessary as long as the Data Privacy Framework exists, it's advisable to do a periodical assessment of the geopolitical situation – especially with regard to the probability of risks occurring – to see if adjusting the risk assessment is necessary.

Loss of control due to a lack of transparency about processing usage data for purposes Salesforce						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	**Current risk**
16.2	Lack of transparency about further processing for purposes Salesforce	Loss of control	**More likely than not**	**Serious**	**High**	
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	**Residual risk**
	Update DPA between HR2day and institutions with: all categories of personal	Update DPA between HR2day and institutions with: all categories of personal data, including usage	**Remote**	**Serious**	**Low**	

	data, including usage data if applicable, HR2day and subprocessors process on behalf of institutions; legitimate business objectives HR2day and subprocessors are allowed to process personal data for and under which conditions; purposes HR2day and subprocessors are not allowed to process personal data for; audit right for institutions with regard to the DPA.	data if applicable, HR2day and subprocessors process on behalf of institutions; legitimate business objectives HR2day and subprocessors are allowed to process personal data for and under which conditions; purposes HR2day and subprocessors are not allowed to process personal data for; audit right for institutions with regard to the DPA.				
	Opt out of providing training data to the global models when using Einstein Search.	Update DPA between HR2day and Salesforce with: all categories of personal data, including usage data if applicable, Salesforce processes on behalf of institutions; legitimate business objectives Salesforce is allowed to process personal data for and under which conditions; purposes Salesforce is not allowed to process personal data for; audit right for institutions with regard to the DPA.				

Inability to exercise data subject access rights to personal data						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	
16.3	Incomplete data subject acces request response.	Inability to exercise data subject access rights to personal data	**More likely than not**	**Serious**	**High**	**Current risk**
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	
		Improve DSAR policy so HR2day is able to provide full access to all personal data they and their subprocessors process.	**Remote**	**Serious**	**Low**	**Residual risk**

Loss of control due to lack of transparency about processing of personal data through cookies						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	

16.4	Incomplete cookie statement/documentation.	Data subjects are unable to inform themselves about processing of personal data through cookies.	**More likely than not**	**Serious**	High	**Current risk**
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	**Residual risk**
		Provide complete cookie statement to all users who use HR2day.	**Remote**	**Serious**	Low	

Loss of control due to having to register for subprocessor updates Salesforce						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	**Current risk**
16.5	Having to register for subprocessor updates Salesforce.	Loss of control.	**Reasonable**	**Serious**	High	
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	**Residual risk**
		Implement a process where HR2day communicates Salesforce subprocessors to institutions.	**Remote**	**Serious**	Low	

General risks

Loss of control due to a lack of transparancy about processing personal data for purposes HR2day						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	
16.6	Lack of transparency about further processing for purposes HR2day	Loss of control	**More likely than not**	**Serious**	**High**	**Current risk**
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	
	Update DPA between HR2day and institutions with: all categories of personal data, including usage data if applicable, HR2day and subprocessors process on behalf of institutions; legitimate business objectives HR2day and subprocessors are allowed to process personal data for and under which conditions; purposes HR2day and subprocessors are not allowed to process personal data for; audit right for institutions with regard to the DPA.	Update DPA between HR2day and institutions with: all categories of personal data, including usage data if applicable, HR2day and subprocessors process on behalf of institutions; legitimate business objectives HR2day and subprocessors are allowed to process personal data for and under which conditions; purposes HR2day and subprocessors are not allowed to process personal data for; audit right for institutions with regard to the DPA. Update privacy statement HR2day.	**Remote**	**Serious**	**Low**	**Residual risk**

Loss of control of user satisfaction data						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	
16.6	Collection of satisfaction data with HR2day as controller for further processing.	Loss of control.	**More likely than not**	**Serious**	**High**	**Current risk**
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	
		Include this processing within the scope of the DPA with HR2day as the processor and give institutions meaningful control (through transparency) and choices in this processing.	**Remote**	**Serious**	**Low**	**Residual risk**

Loss of control and loss of confidentiality by unauthorised access in third countries						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	

16.8	Unauthorised access by parties in third countries.	Loss of control and loss of confidentiality.	**More likely than not**	**Serious**	**High**	**Current risk**
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	**Residual risk**
	Stop using SignRequest.	Identify all transfers, at least to Expo and Google. Include lawful transfers to subprocessors in DPA between HR2day and institution. Inform institutions about parties personal data is being transferred to and they need to conclude agreements with directly. Enable customers who stop using SignRequest to obtain a copy of their data subjects' processed data and delete them when necessary.	**Remote**	**Serious**	**Low**	

Loss of control of subprocessors and recipients through lack of or incorrect agreements						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	**Current risk**
16.9	Lack of or incorrect agreements between HR2day and it's subprocessors.	Loss of control.	**More likely than not**	**Serious**	**High**	**Residual risk**
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	
		Perform assessment if Google and Apple qualify as subprocessors, joint controllers or third party recipients. Include Google and Apple in DPA between HR2day and institutions. Conclude the necessary agreements with Google and Apple.	**Remote**	**Serious**	**Low**	

Loss of confidentiality due to absence of 'read access logging'						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	**Current risk**
16.10	Absence of 'read access logging'	Loss of confidentiality.	**More likely than not**	**Serious**	**High**	

	Measures institution	Measures vendor	Probability	Impact	Risk score	
	Implement 'read access logging' on categories of sensitive and special data at the minimum.	Enable 'read access logging' on categories of sensitive and special data and for the proxy login functionality at the minimum.	**Remote**	**Serious**	**Low**	**Residual risk**
	Implement read access logging for activities administrators carry out using the proxy login.					
	Inform users without undue delay that they have been impersonated.					

Breach of data minimisation by including too broad lists for reasons for absenteeism						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	**Current risk**
16.11	Overly broad (pick) lists for reason of absenteeism.	Breach of data minimisation.	**More likely than not**	**Serious**	**High**	
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	
	Only use a pick lists to collect information about the reason for employees' absence and a fixed set of fields to collect further information about their absence.	Provide instructions to institutions about how to use pick lists to collect sensitive and special categories of data.	**Remote**	**Serious**	**Low**	**Residual risk**
	Have the absenteeism pick list and the fixed set of fields evaluated by the privacy department, to ensure they are in line with GDPR requirement and available guidelines.					
	Ensure users of HR2day are properly instructed and trained about which types of data can be processed about employees' absence.					

Loss of control through open text fields						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	**Current risk**
16.12	Open text fields.	Loss of control.	**More likely than not**	**Serious**	**High**	
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	

	Only use open text fields with a clear purpose.	Provide instructions to institutions about how to use open text fields in a way that respects data minimisation principles.	**Remote**	**Serious**	**Low**	**Residual risk**
	Formulate questions in a way that makes it clear what (sensitive/special) personal data should and shouldn't be provided in an open text field and use the available information icons.	Provide sufficient options for field validation to prevent inaccurate data processing.				
	Ensure users of HR2day are properly instructed and trained about which types of data can be processed in open text fields.					

Lack of accuracy through manual registration of personal data						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	
16.13	Manual registration of personal data.	Lack of accuracy.	**More likely than not**	**Serious**	**High**	**Current risk**
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	
	Automate input where possible, for example by connecting HR2day to the hiring system.	Provide sufficient options for field validation to prevent inaccurate data processing.	**Remote**	**Serious**	**Low**	**Residual risk**
	Ensure HR employees are properly instructed and trained in the institutions' procedures for carefully registering personal data.					

Loss of control of retention periods because of lack of automation						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	
16.14	Lack of automation on enforcing retention periods	Loss of control	**More likely than not**	**Serious**	**High**	**Current risk**
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	

	Determine and manage retention periods for personal data in HR2day.	Provide information and instructions about the procedure to delete data using signal lists to institutions.	**Remote**	**Serious**	**Low**	**Residual risk**
	Ensure the retention periods are complied with by establishing processes to enforce them, for example by using the automated retention periods for documents.	Facilitate institutions in enforcing their retention periods by improving the options for technical configuration and management of retention periods per group of personal data in HR2day.				

Loss of confidentiality due to vertical inheritance of rights default setting						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	**Current risk**
16.15	Vertical inheritence of access rights by default.	Loss of confidentiality.	**Reasonable**	**Serious**	**High**	**Residual risk**
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	
	Turn the vertical inheritance of rights off, unless it's necessary to use this setting.	Proactively inform institutions about the privacy implications of the vertical inheritance of rights setting and offer them the choice to turn it on or off.	**Remote**	**Serious**	**Low**	
	Restrict access to personal data for roles who don't need access to these data to perform their duties.	Cooperate with institutions to improve the options to respect the data minimisation principle while having the vertical inheritance of rights setting on, reducing the administrative burden OR enable them to carry out the necessary workflows while having the setting turned off.				
	Be transparent to data subjects about the usage of the vertical inheritance of rights setting and who has access to their data.					

Loss of control through lack of encryption key management						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	**Current risk**
16.16	Processing of sensitive and special categories of data.	Loss of confidentiality.	**More likely than not**	**Serious**	**High**	
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	

	Assess if cell-level encryption, encryption with customer-managed keys and any other additional measures are necessary for special and sensitive categories of data, taking into account the specific data being processed by the institution and the other security measures in place.	Inform institutions about the encryption methods being used for the HR2day application and platform and about the possibility of additional safeguards, like cell-level encryption and encryption keys managed by HR2day.	**Remote**	**Serious**	**Low**	**Residual risk**
		Cooperate with institutions in assessing the necessary level of encryption for the personal data in HR2day, specifically for the sensitive and special categories of personal data.				
		Where institutions deem it necessary, implement additional safeguards, like cell-level encryption and encryption keys managed by HR2day.				

Mobile app risks

Loss of control of personal data being processed due to installing of mobile app through third-party app store						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	
16.17	Having to download mobile apps from Google and Apple play stores	Loss of control	**More likely than not**	**TBD**	**TBD**	**Current risk**
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	
	Enable access through mobile browser from mobile devices.	Make the app available as side load.	**TBD**	**TBD**	**TBD**	**Residual risk**
	Perform proportionality and subsidiarity assessments on the provision of mobile app via app stores and ‘side-loading’ and implement the results.	Enable access through mobile browser from mobile devices.				

Loss of control due to processing of push notifications by Google and Apple						
Reference	**Cause**	**Consequence**	**Probability**	**Impact**	**Risk score**	**Current risk**
16.18	Having to send push notifications through Google and Apple.	Loss of control	**More likely than not**	**TBD**	**TBD**	
	Measures institution	**Measures vendor**	**Probability**	**Impact**	**Risk score**	**Residual risk**
	Don't include personal data in the messages sent through push notifications.	Optional: Implement unified push for Android users.	**TBD**	**TBD**	**TBD**	
	Perform proportionality and subsidiarity assessments on sending push notifications via Google and Apple or Unified Push and implement the results.					

18 Conclusion

This DPIA has identified sixteen high risks for data subjects and two risks for which the risk level is to be determined . Five of the high risks are related to the use of Salesforce as provider of the platform HR2day runs on. Eleven of the high risks are general risks, caused either by the way institutions (are likely to) use HR2day or by the design of HR2day. Two of the risks are related to use of the mobile app. These two risks exist for any app using app store and push notifications.

Implementing these measures will mitigate all high risks, leaving only low residual risks. Although it is not strictly necessary to mitigate low risks, it is recommended.

All of these risks have a timeline for implementing the measures. Therefore, institutions can continue using HR2day. If the high risks are mitigated, no prior consultation with the data protection authority is required. SURF will publish an update on this DPIA with a conclusion on the implementation of the remaining measures in 2027.

Bijlage 1 Technical Analysis

1.1 Usecases / Scenarios

Involved actors

- Manager 1
- Manager 2
- Employee 1
- Employee 2
- Human Resource Manager

1 **New Employee (Onboarding)**
Actor: HR Manager

1 Create new employee (by HR manager or Manager)
2 Complete the personal information form (including name, address, contact information, emergency contacts)
3 Add consequences disability in record
4 SignRequest Contract
5 Upload required documents (passport/ID card copy)
6 Enter banking information
7 Create a new user (Employee 1) account and set up authentication credentials

2 Self-service : interaction centre
Actors: Employee 1

1 Access personal information/record
~~2 Zoek naar persoonlijke informatie (via zoekfunctie)~~
3 Add emergency contact
4 Download pay slip
5 Submit a leave request
6 Check leave days
7 Change preferred language
8 Fill out mobility form
9 Submit expense claim

3 Self-service management : manager interaction centre
Actor: Manager 1

1 Access and review record of Employee 1
2 Approve/deny leave request of Employee 1
3 Approve mobility form of Employee 1
4 Approve/deny expense claim of Employee 1

4 **Disciplinary action**
Actors: Manager 1, Employee 1, HR Manager 1

Employee 1

1 Provide feedback on co-employee (Employee 2)
2 ~~File complaint on Employee 2.~~

Manager 1

3 Review co-employee performance report (Employee 2)
4 Employee 1 records official complaint against employee 2 Outside HR2day
5 Process a disciplinary action (Employee 2)
6 Transfer employee 2 between departments
7 Instigate a salary adjustment (Employee 2)

HR Manager 1

8 Access and review employee record (Employee 2)
9 Handle an employee complaint/grievance case (Employee 1) Outside HR2day
10 Process a disciplinary action (Employee 2)
11 Handle salary adjustment (Employee 2)

5 Sick leave

Actor: Manager 1

1 Recording sick leave in system (Employee 2)
2 Start reintegration process

6 Reports and exports

Actor: HR Manager 1

1 Report Absentees
2 Report Disability Arrangement
3 Report leave
4 Export report to PDF
5 Export report to Excel

Actor: Manager 1

6 Report Absentees
7 Report Disability Arrangement
8 Report leave
9 Export report to PDF
10 Export report to Excel

1.2 Data Subject Access Request

Data Subject Access Request done by 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-mail adres: ######@#####

Relevante identificatie parameters:
Bijnaam: Gebruiker##############
IP-adres: 62.250.###.###
sr_uuid: ################################
U kunt mij bereiken op: ###############

Tabel 18-1, data subject access request with personal data removed.

Response on the Data Subject Access Request by 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

Talentmanangementgegevens
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)

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, the email received as response on data subject access request with personal data removed.

1.3 Endpoints

An overview of the endpoints that were used during our testing. For the Salesforce endpoints we looked up the designation following the documentation[93] provided to us.

Endpoint	Owner	Description
hr2day-883.lightning.force.com	Salesforce	Salesforce Lightning
hr2day-883.my.salesforce.com	Salesforce	Salesforce login
hr2day-883--hr2d.vf.force.com	Salesforce	Salesforce Visualforce
static.lightning.force.com	Salesforce	Salesforce Lightning
sentry.sr-staging-1.com	SignRequest	No information
SignRequest.com	SignRequest	Website of SignRequest
maps.googleapis.com	Google	Google Maps Api, wordt gebruikt tbv adres opzoeken in declaratie module

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

deu38.sfdc-yzvdd4.salesforce.com	Salesforce	Not specified, in documentation '.salesforce.com' is always mentioned with subdomain '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	Not specified, in documentation. No '.static.' in combination with 'lightning.force.com'.
www.dropbox.com	SignRequest	No information
62vqqh6qv58h.statuspage.io	SignRequest	No information
js.stripe.com	SignRequest	No information
www.googletagmanager.com	SignRequest	No information
login.salesforce.com	Salesforce	Although the URL is obvious it does not appear in documentation.
www.gravatar.com	SignRequest	No information
www.google-analytics.com	SignRequest	No information
SignRequest-pro.s3.amazonaws.com	SignRequest	No information
ajax.googleapis.com	Google	Google API's wordt in combinatie gebruikt met Google Maps API.
cdn.prod.website-files.com	SignRequest	No information
cdnjs.cloudflare.com	SignRequest	No information
d3e54v103j8qbb.cloudfront.net	SignRequest	No information
assets.website-files.com	SignRequest	No information
fonts.googleapis.com	SignRequest	No information
region1.google-analytics.com	SignRequest	No information
consent.cookiebot.com	SignRequest	No information

imgsct.cookiebot.com	SignRequest	No information
fonts.gstatic.com	SignRequest	No information
m.stripe.network	SignRequest	No information
m.stripe.com	SignRequest	No information
hr2day-applanding.herokuapp.com	HR2day	HR2day applanding is used by the HR2day app to determine on which instance URL a user is allowed to log in.
hr2day-883.my.site.com	Salesforce	Salesforce Experience Cloud sites.
csp-report.force.com	Salesforce	Not specified in documentation.
hello.myfonts.net	Onbekend	
hr2day-html2pdf.herokuapp.com	Salesforce	Server where PDF engine resides for generating documents to .pdf

Tabel 18-3, overview of the uncovered endpoints used during our testing.

1.4 Cookies

Cookies HR2day

HR2day places multiple cookies on the users' device. Each of these cookies have a purpose for storing data.

Cookie name	Age	Description
apex__hr2d_MdwSelPic		A yes/no value to remember whether a user wants to see photos of mdw in the mdw employment relationship screen (this is a choice in the UI)
apex__hr2d_MdwSelUD		A yes/no value to remember whether a user wants to see mdws out of service (this is a choice in the UI)
apex__hr2d_reg		Number of lines you want to see on the screen (this is a choice in the UI in many screens)
apex__hr2d_wg		This remembers the last selected employer ID (is a drop-down list in the UI).
apex__hr2d_MdwSelPic		A yes/no value to remember whether a user wants to see photos of mdw in the mdw employment relationship screen (this is a choice in the UI)

apex__hr2d_MdwSelUD		A yes/no value to remember whether a user wants to see mdws out of service (this is a choice in the UI)
apex__hr2d_reg		Number of lines you want to see on the screen (this is a choice in the UI in many screens)
apex__hr2d_wg		This remembers the last selected employer ID (is a drop-down list in the UI).

Tabel 18-4, cookies used by HR2day.

Cookies Salesforce

Salesforce, as the main platform used by HR2day to process it's code, places multiple cookies on the users' device. Each of these cookies have a purpose for storing data.

Cookie name	Age	Description	Info Source
CookieConsentPolicy	1 Year	Used to apply end-user cookie consent preferences set by client-side utility.	SF Documentation
LSKey-c$CookieConsentPolicy	1 Year	Used to apply end-user cookie consent preferences set by our client-side utility.	SF Support
oid	1 Year	Stores the last logged in org for redirecting requests. Used for logging whether the cookie is present in site and community guest-user requests.	SF Support
79eb100099b9a8bf	Session	Browser Fingerprint trigger cookie. Used to detect session security problems.	SF Documentation
RSID		Session ID and login as session ID. Cookies copied to response and cause target URL to rebuild appropriately in a proxy situation.	SF Documentation
SUCSP	Session	Used when the user identity that an admin is assuming, via Log In as Another User, is a Customer Success Portal (CSP) user.	SF Documentation
SUORG	Session	Stores whether you're currently "SU'd" (Switched User) into another user account within your own org.	SF Support

SUPRM	Session	Used when the user identity that an admin is assuming, via Log In as Another User, is a Partner Relationship Management (PRM) portal user.	SF Documentation
clientSrc	Session	Used for security protections.	SF Documentation
inst	Session	Used to redirect requests to an instance when bookmarks/hardcoded URLs send requests to a different instance.	SF Documentation
sid	Session	Session ID used to authenticate Lightning Platform Soap-API and Rest-API data connections for the current user.	SF Documentation
sid_Client	Session	Used to detect and prevent session tampering.	SF Documentation
__Host-ERIC_PROD-<random number>	1 Minute	Enterprise Request Infrastructure Cookie (ERIC) carries the CSRF security token between the server and client. Name indicates server mode (PROD/PRODDEBUG) and a random number. Different token for each Lightning app.	SF Documentation
__Host-ERIC_PRODDEBUG-<random number>		Enterprise Request Infrastructure Cookie (ERIC) carries the CSRF security token between the server and client. Name indicates server mode (PROD/PRODDEBUG) and a random number. Different token for each Lightning app.	SF Documentation
autocomplete	60 Days	Determines if the login page remembers the user's username.	SF Documentation
com.salesforce.LocaleInfo	60 Days	"Stores the locale((language and regional settings)) for login pages. After login its controlled by user settings "	SF Support
disco	Session	Tracks last user login and active session for bypassing login (e.g., OAuth immediate flow).	SF Documentation

lloopch_loid	1 Year	Determines whether to send the user to a specific portal login or an app login.	SF Documentation
lloopch_lpid	1 Year	Stores the last login Portal ID. The cookie is set in frontdoor to send the user to the specified portal login or an app login.	SF Support
login	60 Days	If the user's session has expired, used to fetch the username and populate it on the main login page when using process builder app.	SF Documentation
loginURL	60 Days	Stores the start page for orgs who don't log in using login.salesforce.com	SF Support
oinfo	3 Months	Tracks the last logged in org.	SF Documentation
rememberUn	60 Days	Track the Remember Me checkbox that the user selected to enable login hint.	SF Support
sdtsvalid	Session	Track the Remember Me checkbox that the user selected to enable login hint.	SF Support
setupgtclose	Session	Stores the user's interaction with a guided tour or product walkthrough in the Salesforce Lightning setup interface.	SF Support
sfdc_lv2	1 Year	Stores device activation details for users. If not set or expired, users must verify their identity next login.	SF Support
ak_bmsc	2 hours	Helps protect against malicious website attacks. This cookie is associated with Akamai and is used to differentiate between traffic from humans and bots.	SF Support
bm_sv	2 hours	Helps protect against malicious website attacks	SF Support
Geo	Session	This cookie captures the user's geographic location, including continent, country, state, and city. Cookie is available for static.lightning.force.com domain.	SF Support

52609e00b7ee307e	Session	Browser Fingerprint cookie. Used to detect session security problems.	SF Support
embeddedcomponentcalloutcookie	Session	embeddedcomponentcalloutcookie serves as a flag cookie to control whether a particular UI callout (guided tour popup) related to Analytics embedded components should be shown to the user or not.	SF Support
setupprofileheadergt	Session	cookies that manage various aspects of the Guided Tour functionality that is interactive tours designed to help new users understand specific features.	SF Support
setupprofileobjectsandtabsgt	Session	Tracks user interaction with a guided tour focused on the Objects and Tabs settings under user profiles.	SF Support
unifiedsearchgt	Session	Tracks guided tour status for the Unified Search experience	SF Support

Tabel 18-5 cookies uses by Salesforce, details partly from cookie documentation Salesforce[94] (SF Documentation) partly from feedback salesforce support and via HR2day (SF Support).

Cookies SignRequest

SignRequest, is the sub-processor used by HR2day to handle its digital signing of documents, places multiple cookies on the users' device. Each of these cookies have a purpose for storing data.

Cookie name	Age	Description
_cfuvid		No documentation
csrftoken		No documentation
sessionid		No documentation
sr_user_tags		No documentation
sr_uuid		No documentation
m		No documentation

Tabel 18-6, cookies placed by SignRequest.

Unknown 3rd Party Cookies

Cookie name	Age	Owner	Description
__cf_bm		Myfonts.net	No documentation

Tabel 18-7, cookies placed by 3rd parties.

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

1.5 Logging datasets

Login History
In reference to 4.3.10.2.

Field	Description
Username	The name of the user who logged in.
Login time	Formatted date and time (CET) when the login occurred.
Source IP	IP address from which the user logged in; shows proxy/load balancer IP if applicable.
Login type	How the login was performed, e.g., via HR2day login screen or SSO.
Status	Indicates if login succeeded and failure reasons if applicable.
Browser	Browser used by the user to log in.
Platform	Platform used during login, e.g., Windows or Mac.
Application	Application or interface used to log in to Salesforce (HR2day).
Client version	Version of the client application if multiple versions exist.
API type	Type of API used if login was via API user.
API version	API version used if login was via API user.
Login URL	URL where the login was performed.
Environment	To what environment the login took place.
TLS protocol	TLS protocol version used during login.
TLS Cipher Suite	TLS cipher suite used during login.
Country code	Country code from where the login originated.
Country	Country from where the login originated.
Subdivision	Province or state from where the login occurred.
City	City from where the login originated.
Postal code	Postal code from where the login originated.
Latitude	Latitude coordinate of login location.

Longitude	Longitude coordinate of login location.
HTTP method	HTTP method used during login.
Authentication method reference	Indicates if/how authentication was delegated to an external identity provider.
Login subtype	Detailed information on the login method, e.g., OAuth or API usage.
Forwarded for IP	IP address of user if login was via intermediary like proxy or load balancer.

Tabel 18-8, processed personal data in login history logging.

Event logging - Login
In reference to 4.3.10.3

Field	Description
EVENT_TYPE	This is always Login here.
TIMESTAMP	Shows the login time (timezone GMT) in ISO 8601 format without separators, with milliseconds added: YYYYMMDDHHmmSSsss.
REQUEST_ID	A unique Salesforce ID that identifies the login transaction.
ORGANIZATION_ID	A unique Salesforce ID that identifies the Salesforce environment being logged into.
USER_ID	A unique Salesforce ID that identifies the user who logs in.
RUN_TIME	The amount of time in milliseconds required to complete the request.
CPU_TIME	The amount of CPU time in milliseconds required to complete the request.
URL	The address to which the user sent the login request.
SESSION_KEY	The unique session ID of the user.
LOGIN_KEY	A unique string linking all events within a user's login session, starting with login and ending with logout or session expiration.
USER_TYPE	Displays the license type of the user who is logging in. Possible values: CsOnly, CspLitePortal, CustomerSuccess, Guest, PowerCustomerSuccess, PowerPartner, SelfService, Standard.
REQUEST_STATUS	Indicates whether login was successful. Possible values: S: success, F: failure, U: undefined, A: authorization failure, R: redirect, N: not found.

DB_TOTAL_TIME	The total time in nanoseconds required for a database roundtrip.
LOGIN_TYPE	Shows the method used to log in. Possible values: 7 : AppExchange, A : Application, s : Certificate-based login, k : Chatter Communities External User, n: Chatter Communities External User Third Party SSO, x: Cross Tenant Login (internal use), r: Employee Login to Community, z: Lightning Login, l: Networks Portal API Only, 6: Remote Access Client, i: Remote Access 2.0, I: Other Apex API, R: Partner Product, w: Passwordless Login, 3: Customer Service Portal, q: Partner Portal Third-Party SSO, 9: Partner Portal, 5: SAML IdP Initiated SSO, m: SAML Chatter Communities External User SSO, b: SAML Customer Service Portal SSO, c: SAML Partner Portal SSO, h: SAML Site SSO, 8: SAML Sfdc Initiated SSO, E: SelfService, j: Third Party SSO.
BROWSER_TYPE	Shows the type and version of the browser used during login.
API_TYPE	Displays the type of API used during login. Possible values: 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	Displays the version of the API used during login.
USER_NAME	The name of the user logging in.
TLS_PROTOCOL	Shows the TLS protocol used during login.
CIPHER_SUITE	Shows the specific encryption algorithms used to secure the connection.
LOGIN_URL	Displays the URL where the user sent the login request.
AUTHENTICATION_METHOD_REFERENCE	Indicates the authentication method used (e.g., standard, SAML, OIDC, or multi-factor authentication).
LOGIN_SUB_TYPE	The flow used for login. Possible values: authClientCredentials: OAuth Client Credentials, OauthHybridRefreshToken: OAuth Refresh Token for Hybrid Apps, OauthHybridTokenExchange: OAuth Token Exchange for Hybrid Apps, OauthHybridUserAgent: OAuth User-Agent for Hybrid Apps, OauthHybridWebServer: OAuth Web Server for Hybrid Apps, OauthOtpLogin: OAuth OTP Login, OauthRefreshToken: OAuth Refresh Token, OauthTokenExchange: OAuth Token Exchange, OauthUserAgent: OAuth User-Agent, OauthUserAgentIdToken: OAuth User-Agent with ID Token, OauthUsernamePassword: OAuth Username-Password, OauthWebServer: OAuth Web Server, UiPasswordReset: UI Password Reset, UsernamePasswordUiLogin: UI Username-Password.

AUTHENTICATION_SERVICE_ID	Displays a unique identification code referring to the specific authentication service used during login.
TIMESTAMP_DERIVED	ISO 8601 format with separators and milliseconds added: YYYY-MM-DDTHH:mm:SS.sssZ.
USER_ID_DERIVED	The user ID of the logged-in user, case-insensitive.
CLIENT_IP	Displays the IP address of the user logging in.
URI_ID_DERIVED	Shows the Salesforce ID of the URL receiving the login request.
LOGIN_STATUS	Indicates whether the login was successful or not.
SOURCE_IP	The IP address of the device that submitted the login request. May be a proxy or intermediary device.
FORWARDED_FOR_IP	The original IP address of the device where the login originated.

Tabel 18-9, processed personal data in event logging on login.

Event logging logout
In reference to 4.3.10.3

Field	Description
EVENT_TYPE	This is always Logout here.
TIMESTAMP	Shows the logout time (timezone GMT) in ISO 8601 format without separators, with milliseconds added: YYYYMMDDHHmmSSsss.
REQUEST_ID	Unique Salesforce ID that identifies the logout transaction.
ORGANIZATION_ID	Unique Salesforce ID that identifies the Salesforce environment being logged out from.
USER_ID	Unique Salesforce ID that identifies the user who logs out.
USER_TYPE	Shows the type of user logging out. Possible values: A : Automated Process, b : High Volume Portal, C : Customer Portal User, D : External Who, F : Self-Service, G : Guest, L : Package License Manager, N : Salesforce to Salesforce, n : CSN Only, O : Power Custom, o : Custom, P : Partner, p : Customer Portal Manager, S : Standard, X : Salesforce Administrator.
SESSION_TYPE	The session type that was in use when logging out. Possible values: A: API, I: APIOnlyUser, N: ChatterNetworks, Z: ChatterNetworksAPIOnly, C: Content, P: OauthApprovalUI, O: Oauth2, T: SiteStudio, R: SitePreview, S : SubstituteUser, B: TempContentExchange, G:

	TempOauthAccessTokenFrontdoor, Y: TempVisualforceExchange, F: TempUIFrontdoor, U: UI, E: UserSite, V: Visualforce, W: WDC API.
SESSION_LEVEL	Session security level in use during logout (value 1 means standard session, 10 means high-assurance session).
BROWSER_TYPE	Browser that was used during logout.
PLATFORM_TYPE	Platform used by the user. If the logout occurred due to timeout, the value is null. Possible values: 1000: Windows, 1008: Windows 2003, 1013: Windows 8.1, 1015: Windows 10, 2003: Macintosh/Apple OSX, 4000: Linux, 5005: Android, 5006: iPhone, 5007: iPad, 5200: Android 10.0.
RESOLUTION_TYPE	User's screen resolution at the time of logout. If logout occurred due to timeout, the value is null.
APP_TYPE	The application type that was in use during logout. Possible values: 1000: Application, 1007: SFDC Application, 1014: Chat, 2501: CTI, 2514: OAuth, 3475: SFDC Partner Portal.
CLIENT_VERSION	The version of the client that was in use during logout.
API_TYPE	The type of API request. Possible values: 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	The version of the API that was used.
USER_INITIATED_LOGOUT	Returns the value 1 if the user explicitly logged out using the logout button; in all other cases (timeout, browser close), the value is 0.
SESSION_KEY	Unique session ID of the user.
LOGIN_KEY	A unique string linking all events within a user's login session, beginning with a login event and ending with a logout event or session expiration.
TIMESTAMP_DERIVED	ISO 8601 format with separators and milliseconds added: YYYY-MM-DDTHH:mm:SS.sssZ.
USER_ID_DERIVED	User ID of the logged-out user; unlike USER_ID, this is case-insensitive.
CLIENT_IP	IP address of the user logging out.

Tabel 18-10, all data processed in event logging type logout.

Event logging hostname redirects

In reference to 4.3.10.3

Field	Description
EVENT_TYPE	This is always '*HostnameRedirects'* here.
TIMESTAMP	Shows the time (timezone GMT) of the redirect in ISO 8601 format without separators, with milliseconds added: YYYYMMDDHHmmSSsss.
REQUEST_ID	Unique Salesforce ID of the redirect.
ORGANIZATION_ID	A unique Salesforce ID that identifies the Salesforce environment where the redirect occurs.
USER_ID	A unique Salesforce ID that identifies the user being redirected.
RUN_TIME	Not used in the redirect; therefore always 0.
CPU_TIME	Not used in the redirect; therefore, always Null.
URL	Not used in the redirect; therefore, always Null.
SESSION_KEY	Not used in the redirect; therefore, always Null.
LOGIN_KEY	Not used in the redirect; therefore, always Null.
MESSAGE	Not used in the redirect; therefore, always Null.
DOMAIN	Not used in the redirect; therefore, always Null.
SOURCE_HOSTNAME	This is the hostname from which the redirect originates.
TARGET_HOSTNAME	The hostname to which the user is redirected.
PATH	The path of the original URL request, up to the first question mark (?). The path is also used in the target URL of the redirect. However, this field does not include any query string if present.
REDIRECT_REASON	Indicates the reason for the redirect. Possible values: Redirected due to a hostname mismatch; Redirection suppressed to prevent Lightning Out integration failure; Redirection was blocked because redirections for this hostname are disabled; Redirection was blocked because redirections for the legacy SOURCE_HOSTNAME are no longer supported.
REDIRECT_IS_BLOCKED	Indicates whether the redirect succeeded (value 0) or was blocked (value 1).
REFERRER	The absolute or partial address from which the request to the SOURCE_HOSTNAME originated.

ORIGIN	The origin (protocol, hostname, and port) that triggered the request to the SOURCE_HOSTNAME.
TIMESTAMP_DERIVED	ISO 8601 format with separators and milliseconds added: YYYY-MM-DDTHH:mm:SS.sssZ.
USER_ID_DERIVED	The user ID of the redirected user; unlike USER_ID, this field is case-insensitive.
CLIENT_IP	Displays the IP address of the user being redirected.
URL_ID_DERIVED	Not used in the redirect; therefore always Null.

Tabel 18-11, event logging type hostname redirects.

Event logging CSP violations
In reference to 4.3.10.3

Field	Description
EVENT_TYPE	This is always CSPViolation here.
TIMESTAMP	Shows the time (timezone GMT) of the request in ISO 8601 format without separators, with milliseconds added: YYYYMMDDHHmmSSsss.
REQUEST_ID	Unique Salesforce ID of the transaction.
BLOCKED_URI	The full string of the blocked resource. If the blocked resource request used a URL, BLOCKED_URI is the full URL.
BLOCKED_URI_DOMAIN	If BLOCKED_URI is a URL, this contains the domain of that URL.
DIRECTIVE	The CSP directive that blocked the resource request. Possible values: font-src, frame-src, img-src, media-src, style-src, unsafe-eval, unsafe-inline.
CONTEXT	CSP violation events capture details only about blocked resource requests from Lightning Experience pages. This value is therefore always “Lightning.”
UNIQUE_ID	Unique Salesforce ID of the event.
DISPOSITION	The instructions for how the user agent handled the CSP violation at the time it occurred. Possible values: *enforce:* the request was blocked *report:* the request was not blocked but was reported.
SOURCE	The page where the CSP violation originated.

COLUMN_NUMBER	The column number in the document or script where the violation occurred. This value is only relevant when the DIRECTIVE is unsafe-eval or unsafe-inline. Use this together with LINE_NUMBER to identify the violation's location.
LINE_NUMBER	The line number in the document or script where the violation occurred. This value is only relevant when the DIRECTIVE is unsafe-eval or unsafe-inline. Use this together with COLUMN_NUMBER to locate the violation.
SOURCE_FILE	The URL of the script where the violation occurred. If the violation did not occur in a script, SOURCE_FILE is null.
RESOURCE_SAMPLE	A sample of the resource that caused the violation, usually the first 40 characters or an empty string.
TIMESTAMP_DERIVED	ISO 8601 format with separators and milliseconds added: YYYY-MM-DDTHH:mm:SS.sssZ.

Tabel 18-12, event logging type CSP violation.

Event logging API total usage

In reference to 4.3.10.3

Field	English Translation
EVENT_TYPE	This is always ApiTotalUsage here.
TIMESTAMP	Shows the time (timezone GMT) of the API request in ISO 8601 format without separators, with milliseconds added: YYYYMMDDHHmmSSsss.
REQUEST_ID	Unique Salesforce ID of the transaction.
ORGANIZATION_ID	A unique Salesforce ID that identifies the Salesforce environment where the API request occurs.
USER_ID	A unique Salesforce ID that identifies the API user submitting the request.
API_FAMILY	The type of API being used; for example, Rest, Soap, or Bulk.
API_VERSION	Shows the version of the API that was used.
API_RESOURCE	The API method or resource.
CLIENT_NAME	The name of the client that submitted the API request.
HTTP_METHOD	The HTTP method, e.g., GET.

CLIENT_IP	The IP address of the client using Salesforce services. An internal Salesforce IP address (for example, a login from AppExchange) appears as “Salesforce.com IP.”
COUNTS_AGAINST_API_LIMIT	Indicates whether the request counts toward the API limit (true) or not (false).
CONNECTED_APP_ID	The name of the connected app that made the API request.
ENTITY_NAME	The name of the Salesforce object that the API request attempted to access.
STATUS_CODE	The HTTP response status code for the request.
CONNECTED_APP_NAME	The name of the connected app that made the API request.
USER_NAME	The username of the API user in Salesforce.
TIMESTAMP_DERIVED	ISO 8601 format with separators and milliseconds added: YYYY-MM-DDTHH:mm:SS.sssZ.

Tabel 18-13, event logging type API total usage.

Event logging Apex Unexpected Exceptions
In reference to 4.3.10.3

Field	Description
EVENT_TYPE	This is always ApexUnexpectedException here.
TIMESTAMP	Shows the time (timezone GMT) of the error in ISO 8601 format without separators, with milliseconds added: YYYYMMDDHHmmSSsss.
REQUEST_ID	Unique Salesforce ID of the error.
ORGANIZATION_ID	A unique Salesforce ID that identifies the Salesforce environment where the error occurred.
USER_ID	A unique Salesforce ID that identifies the user performing the action that caused the error.
EXCEPTION_TYPE	The class type of the error.
EXCEPTION_MESSAGE	The content of the error message.
STACK_TRACE	The stack trace of the error.
EXCEPTION_CATEGORY	The category of the error, indicating if a limit such as heapsize or CPU time was exceeded. Possible values: LimitException: CpuTime, LimitException: HeapSize, LimitException: Queries, LimitException: QueryRows, LimitException: DmlStatements, LimitException: Callouts.

TIMESTAMP_DERIVED	ISO 8601 format with separators and milliseconds added: YYYYMMDDHHmmSSsss.
USER_ID_DERIVED	The user ID of the logged-in user; unlike USER_ID, this is case-insensitive.

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

Change History Tracing
In reference to 4.3.10.4.

Object	Description
Afdeling	Department Number, Start Date, Parent Department, End Date, Email, Delegated Manager, House Number, Cost Centre, Manager, Name/Code, Description, Signatory Department Name, Signatory With, Signatory Title, City, Postal Code, Phone, Street, Employer, and Website
Arbeidsrelatie	Start of Employment Relationship, Department, Single Parent Allowance, Employment Conditions Group, Car, Car Value, Bank 2 IBAN, Pension Participation 1, Part-time Percentage, End of Employment Relationship, Position, Valid Until, Valid From, Wage Tax Reduction, Schedule, Salary, Salary Scale, Step, Hourly Wage, and Changes
Arbeidsrelatiewijziging	Start of Employment Relationship, Single Parent Allowance, Date Processed, and Explanation
Declaratiecategorie	Employment Conditions Cluster, Declaration Category, Wage Component Definition, Description, Process Definition Code, Type, and Variant
Declaratiecategorie Runtime	Employment Conditions Cluster, Wage Component Definition, Description, Process Definition Code, Type, and Variant
Document Signflow Ondertekenaar	Phone (not in use)
Kostenplaats	Start Date, Budget Holder, Dimension, End Date, Delegated Budget Holder, Name/Code, Description, Aggregation Characteristic, and Employer
LooncompDefinitie	Quantity, Quantity Parameter, Wage Component to Split, Code, Owner, Factor, Factor Parameter, Basis, Index, Cost Distribution, Wage Component, Payslip Options, Description, Options, Pro Rata, Scheme, General Ledger Classification, Rate, Rate Parameter, and Type
Looncomponent	Quantity, Account, Bank Description, Account Holder Name, Bank IBAN, Bank Account, Amount, Factor, Valid Until, Valid From, Cost Center, Cost Center Dim2, Cost Center Dim3, Wage Component Definition, Wage Component Name, Reference, and Rate

Medew/HR gegevens	Bank IBAN, Marital Status, Date of Employment, Date of Termination, Private Email, House Number Addition, House Number, Name, Postal House Number Addition, Postal House Number, Postal Code, Postal Street, Postal City, Postal Code, Street, Phone, Phone 2, and City
Medew/HR gegevens wijziging	Date Processed, Status, and Explanation
MessageInfo	Date Rejected, Date Accepted, Date Sent, Last Check Attempt, Last Send Attempt, and Status
Opleidingswijziging	Date Processed
Review	Approval Employee 1, Approval Employee 2, and Approval Employee 3
SignRequest	Status
Werkgever	Employment Conditions Cluster, Bank IBAN, Email, Financial Admin ID, GL Account Scheme, Year, Wage Tax Number, Payroll TWK Previous Year, Pension Fund Number, and Status

Tabel 18-15, data processed by default in Change History Tracing, keep in mind that the selected object can log up to 20 fields.

Debug logging
In reference to 4.3.10.5

Dutch Term	English Translation
Execution Units	the transaction a user performs in HR2day.
Code Units	Individual unit of work within a transaction. Code units include, for example, Triggers, Validation Rules, Webservice calls, Visualforce actions on Apex controllers, etc.
Log Entries	Log extract showing a wide variety of event types, for instance SQL queries, separated by a pipe (|).
Timestamp	The time the event occurred, in the format HH:mm:ss.SSS. In parentheses behind it is the value in nanoseconds that has elapsed since the start of the request.
Event indicator	The event that triggered the debug log entry. This includes additional data (code) captured with the event, such as the method name or the line and character number where the code was executed.
Cumulative resource usage	Shows the summed consumption of system resources during code execution.

Cumulative profiling information	Recorded at the end of the transaction and contains information about DML calls, expensive queries, and such.
Version	API version used during the transaction.
Log category	Type of information captured.
Log level	The amount of information captured.

Tabel 18-16, data processed by debug logging.

Setup Audit Trail
In reference to 4.3.10.6

Field	Description
User	User who made the change
Timestamp	Time of the modification
Type of change	Type of change (for example: new field, workflow adjusted)
Details	Details of what was changed exactly
IP address	IP address from which the change originated
Session information	Session information

Tabel 18-17, data processed by Setup Audit Trail.

Email Logs
In reference to 4.3.10.7

Dutch Term (translated)	English Translation
Date/Time	Date/Time of sending/receiving the email
Internal message ID	Unique Salesforce ID of the email
Mail event	Code of the event. Possible values: R - Reception: The email was successfully received D - Delivery: The email was successfully sent T - Temporary failure: The email delivery was delayed. Salesforce will retry sending it. P - Permanent failure: The email could not be delivered
Recipient	Email address of the recipient
Sender	The “Envelope From” address used in the email message

External Host	IP address of the application server that delivered the email to the mail server
Bytes Transferred	Size of the email message
Salesforce.com user	Salesforce ID of the user who sent the email
Message header ID	Message ID header at the beginning of each email
Retry count	Number of attempts made to deliver the email
Seconds in queue	Number of seconds the email waited before delivery
Delivery phase	Delivery phase and error message if sending failed
Forwarding address	Hostname of the designated relay system
Forwarding port	Port of the designated relay system
Delivery status notification	Per phase, a three-digit response code returned by the mail server
TLS Cipher	Encryption used for the email message
TLS Verified	Indicates whether the email message was verified or not
SPF status	Authentication status of the email message via the Sender Policy Framework (SPF)
Sender ID status	Authentication status of the sender ID of the email message
PRA Sender ID status	Purported Responsible Address authentication status of the sender ID of the email message
DomainKeys status	DomainKeys status of the email message
Header From	The “From” field in the email header
DKIM selector	DKIM selector of the email message
DKIM domain	DKIM domain associated with the DKIM signature
DKIM passed	Indicates whether the DKIM signature header was included in the email headers

Tabel 18-18, data processed in Email Logs.

1.6 HR2day App Push Notifications

This chapter describes the possible push notifications that are displayed in the HR2day app.

Based on the selected code, here is a detailed description of the possible notifications, including the exact text content and parameters.

Notifications for the employee

Here are the different notification types that an employee can receive with their exact text content:
Document notifications

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

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

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

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

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

New Document (General)
- 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} = Object type label (bijv. "Declaratie", "Functioneringsgesprek")

New File
- 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

Declaration notifications

Claim Approved
- 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

Declaration Rejected
- Nederlands: "Je declaratie is afgekeurd"
- Engels: "Your declaration has been denied"
- Body Nederlands: "Reden: {0}"
- Body Engels: "Reason: {0}"
- Parameters: {0} = Reden van afwijzing

Declaration processed
- 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

Leave Management

Leave Approved
- 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)

Leave Rejected
- 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)

Performance reviews

Appraisal requested
- 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 review string (bijv. "functioneringsgesprek")

Process Management

Process Instance Approved
- Nederlands: "Je wijziging is goedgekeurd"
- Engels: "Your change has been approved"
- Body: Naam van de procesinstantie
- Parameters: Geen

Processing Authority Rejected
- 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 karakters)

General Notifications

Signing the document
- 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

New Alert
- Nederlands: "Er is een nieuwe openstaande actie"
- Engels: "There is a new open action"
- Body: Alerttekst
- Parameters: Geen (body komt uit alert record)

New Announcement
- Nederlands: "Er is een nieuwe mededeling"
- Engels: "There is a new announcement"
- Body: Naam van de mededeling
- Parameters: Geen

New Questionnaire
- Nederlands: "Er is een nieuwe vragenlijst"
- Engels: "There is a new survey"
- Body: Naam van de vragenlijst
- Parameters: Geen

Notifications for the manager

Leave requests

Leave request submitted
- 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

General Changes (via Process Engine)

Template for All Change Types
- 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

Employment relationship change
- Nederlands: "Arbeidsrelatiewijziging"
- Engels: "Employment relationship change"
- Trigger: Via ProcessAssignment voor hr2d__ArbeidsrelatieChange__c

Declaratie (via Proces Engine)
- Nederlands: "Declaratie"
- Engels: "Declaration"
- Trigger: Via ProcessAssignment voor hr2d__Declaration__c

Employee change
- Nederlands: "Medewerkerwijziging"
- Engels: "Employee change"
- Trigger: Via ProcessAssignment voor hr2d__EmployeeChange__c

Wage component change
- Nederlands: "Looncomponentwijziging"
- Engels: "Wage type change"
- Trigger: Via ProcessAssignment voor hr2d__LooncompOutputChange__c

Qualification
- Nederlands: "Kwalificatie"
- Engels: "Qualification"
- Trigger: Via ProcessAssignment voor hr2d__Qualification__c

Leave scheme recording
- Nederlands: "Verlofregeling opname"
- Engels: "Leave scheme booking"
- Trigger: Via ProcessAssignment voor hr2d__LeaveSchemeBooking__c

Training change
- Nederlands: "Opleidingswijziging"
- Engels: "Education history change"
- Trigger: Via ProcessAssignment voor hr2d__EducationHistoryChange__c

Expense claims (Old Flow)
Claim Submitted (Legacy)
- Onderwerp: "Declaratie" (gebruikt CHANGE_SUBMITTED_SUBJECT template)
- 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

Training changes (Legacy Flow)
Training change per Approval Step
- 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

Technical Details

Localisation
- Supported languages: Dutch (nl_NL) and English (en_US)
- Default: Dutch is used as a fallback for unsupported locales
- Language determination: Automatic based on employee locale settings

Parameter replacement
- Parameters are replaced using the `String.format()` method
- Placeholders use {0}, {1}, {2} etc. notation
- Dates are formatted with the `.format()` method
- Some parameters have logic for single-day vs. multi-day leave

Bijlage 2 Data categories

Directly identifiable data
This is data used to uniquely identify (and authenticate/authorise) a person. Examples include name (first name, surname), date and place of birth, citizen service number (BSN), passport or ID number and biometric data (such as fingerprints or facial recognition).

Contact data
This data is used to contact a person. Examples include: email address, telephone number (landline and mobile), postal address and social media accounts.

Demographic data
This is data that describes the general characteristics of a person. Examples include age, gender, nationality, marital status, level of education and occupation or position.

Organisation data
This data relates to the organisation with which a person is affiliated. Examples include company name, job title, department, work address, business email address and telephone number.

Technical data
This data relates to the technical aspects of the use of devices and services. Examples include device IDs, browser type and version, operating system, cookie data, log files and usage statistics of apps or websites.

Financial data
Data revealing information about someone’s financial situation.

Special categories of data
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. This data is highly sensitive and is subject to a separate interpretation in the GDPR.