TalentRadar

fact sheet

Randstad Enterprise believes in ensuring that our client data is protected, secured, and properly stored and removed throughout the lifecycle of the partnership. Randstad Enterprise also believes transparency is key in establishing trust with our clients to build and maintain lasting relationships. Below is a list of questions and answers that provide insight into how Randstad Enterprise provides protection and trust for the client's end-to-end data processing

data encryption and retention

Is data encrypted in transit?	Yes, data in transit is encrypted. (TLS 1.2)
Is data encrypted at rest?	Yes, data at rest is encrypted. (AES 256-bit)
Does anyone have direct access to the data once it lands in TalentRadar and could it be edited?	Only the randstad BI team managing the data pipeline and dashboards will have access to the data.
How long is data retained in TalentRadar?	Data retention: - personal data 5y or end of the contract, whatever occurs first. - non-personal data, during the lifetime of the contract.
How is the data past retention disposed of?	Data past the retention period are purged from TalentRadar (Domo & GCP) storage resources.

security logging & monitoring

What logging is in place for Talent Radar?	All activity in TalentRadar is logged in the activity log, and accessible but not editable by the randstad data governance team admins. This includes administrative activities, user access management and audit logs. A full list of logging details is available upon request.
How long are these logs retained?	Security logs are retained for 180 days
Who has access to these logs, and can they be deleted?	The administrators in the data governance team have read access rights on the logs, but log entries cannot be edited or deleted.
What personal information is stored in the logs?	Only the personal information of the registered user is stored in the logs (name, email).

user access & authentication

How do admins authenticate to Talent Radar?	All randstad enterprise employees, including administrators login via the randstad corporate SSO (OpenID).
Is there an MFA in place?	All randstad employees authenticate using Randstad's corporate SSO platform, which requires MFA authentication. Additionally, users created on the Domo instance are authenticated with username and pw and a 2nd factor (usually SMS sent to the user's mobile number).
Is there an access requesting process between the client RSR for admin access when needed?	Yes, we have users and access management processes in place. All accesses are requested via the randstad ticketing system by the account leader, who is responsible for the users with access to their accounts.
How long would RSR retain admin access to the client instance in the event of being granted it?	During the lifetime of the client contract, TalentRadar instance is managed by randstad, client users are considered information consumers. At the contract end, the data purging policy will be applied, including the purging of the client instance as a whole.
Are access reviews conducted on admin access?	Yes, administrators are all within the data governance team; when people change roles or leave the company, they are removed from TalentRadar (remove user process in attachment), and since we work with SSO, employees who leave lose access by default. On top of that, we do quarterly reviews of the admin accesses.

data protection & storage

Where is the data stored?	Clients can choose to store their data in one of the following data center locations. All data from the client will be stored in the same data center: US, EU, Australia, Japan.
Are the environments adequately protected?	The following controls are put in place to protect the security of the environment:: - Data Encryption - Firewalls - OS hardening - Device decommissioning - Vulnerability scanning and management - Third-party penetration testing - Access management - Password management - Endpoint management - Incident management - System Development and maintenance/Change Management - Patch management - Availability management - Input and output validation
Does the system depend on any single point of failure?	RDS database backups are automatically stored as snapshots in the AWS infrastructure daily. These database snapshots are stored in AWS S3. In case of an RDS instance failure, AWS detects failure and automatically fails over to the backup instance. current GCP applications for processing data uses 2 main storage units: Cloud sql, Bigquery By default: Cloud SQL retains seven automated backups, in addition to on-demand backups. BigQuery offers a feature called ‘time travel’, allowing us to access the table's historical versions in the past seven days.

How do we ensure secure config, cloud security standards, patching, etc, is in place?	Managing the cloud infrastructure and the technology stack under TalentRadar is Domo's responsibility. Domo maintains an information security program compliant with ISO 27001 and SOC 2 and operates security controls according to the highest standards. randstad and its vendors follow security standards and best practices. Production systems are built from preconfigured and hardened images that are reviewed and approved by Domo's information security team. Approval requires adherence to Domo's enterprise security configuration standards.