iris

SAMPLE REPORT · DEMO DATA

Sensitive-data evidence report

What was scanned, what was found, who can reach it, and what could not be checked.
Every finding links to its source table and column.

1 Scope record

Organization	Example Organization (demo tenant; all records are synthetic)
Source scanned	`enterprise_data` · database · 2 schemas (`iris_dataset` , `public`)
Objects in scope	16 tables · 190 columns
Scan	26 October 2026, 15:05–15:09 · operation `cd75f96d` · status completed
Access mode	Read-only connection. IRIS made no changes to the source.
Scan history	22 completed scans of this source between 18 Sep and 26 Oct 2026

2 Summary

875.3K
rows scanned

70
of 190 columns hold personal or sensitive data

497.4K
sensitive values matched

2
open access findings (1 critical)

Data types found include names, email addresses, phone numbers, dates of birth, passport and driving-license numbers, payment-card and bank-account numbers, health information, and system credentials, plus regional identifiers.

3 Coverage and explicit gaps

Empty table, values not checked. `marketing_contacts` returned 0 rows. Its columns (`first_name` , `last_name` , `email` , `phone`) were classified from column names and types only. Re-scan once the table holds data.

Classifications awaiting review. Most results are machine verdicts. A reviewer has not yet confirmed them; each row in IRIS shows its review status and confidence score.

Subject-request search not run. No data subject access request (DSAR) search has been run against this source, so DSAR impact is recorded as "not searched".

4 Key findings

System credentials stored without protection

Critical

In `user_credentials`, passwords appear hashed, but API keys and MFA secrets sit next to them with no protection detected.

Evidence: `api_key` · Credential · 96% · protection: none detected | `mfa_secret` · Credential · 96% · none detected | `password_hash` · Credential · 96% · appears hashed. 15 rows.

Next step: the application owner rotates the exposed keys and secrets and moves them to a secrets store. Re-scan to confirm the condition changed.

Payment and bank data inside the HR system

Critical

The employee table holds payment-card and bank-account numbers in clear text.

Evidence: `hrms_employees.credit_card_number` · Credit card · 88% | `hrms_employees.bank_account_number` · Bank account · 88%. Protection: none detected. 200,000 rows.

Next step: confirm a business need. If there is none, remove the data; if there is, restrict access and protect the columns.

Health information outside a health system

High

Medical conditions and allergies are stored in the general HR table.

Evidence: `hrms_employees.medical_conditions` · Medical record · 92% | `hrms_employees.allergies` · Allergies · 87%. Protection: none detected. 200,000 rows.

Next step: the HR data owner confirms the purpose and who needs access; apply the retention rule for health data.

Identity documents in clear text

High

Passport and driving-license numbers are stored without protection.

Evidence: `hrms_employees.passport_number` · Passport · 94% | `hrms_employees.driving_license` · Driving license · 94%. Protection: none detected. 200,000 rows.

Next step: mask the columns for non-HR users; record the decision in IRIS.

Access that is no longer used

Medium

One account can reach sensitive data it has not used in the review period.

Evidence: principal `enterprise_user` (user) · 2,024 sensitive objects · last detected 26 Oct 2026, 15:09 · status open.

Next step: the source owner reviews the account and removes access that is not needed. A re-scan records the result.

Confidence is IRIS's score for each classification before human review. "Protection" shows whether values appear encrypted, masked or hashed, based on sampled values.

5 Evidence register (excerpt)

Each item is generated from scan data and mapped to a control in IRIS's unified control framework, which links to GDPR, CCPA/CPRA, HIPAA and the other supported frameworks. Items stay "under review" until a person approves them.

EVIDENCE ITEM	CONTROL	TYPE	ORIGIN	REVIEW	VALIDITY
Classification report	`CF5-005`	Technical documentation	IRIS-generated	Under review	Valid
Sensitivity classification	`CF2-008`	Technical documentation	IRIS-generated	Under review	Valid
Privileged access detection	`CF1-005`	Technical documentation	IRIS-generated	Under review	Valid
User provisioning report	`CF1-007`	Technical documentation	IRIS-generated	Under review	Valid
Right to erasure assessment	`CF4-003`	Technical documentation	IRIS-generated	Under review	Valid
Data retention policy	`CF6-001`	Policy document	IRIS-generated	Under review	Valid
Incident logging assessment	`CF7-002`	Audit report	IRIS-generated	Under review	Valid
Record of processing configuration	`CF8-005`	Policy document	IRIS-generated	Under review	Valid

The full register exports from IRIS as CSV or XLSX, with the generated date, scope, reviewer decision and expiry for each item.

6 Re-scan record

A closed ticket isn't proof that the risk changed. After the owners act on section 4, a re-scan of the same scope records the new condition next to this one, with both scans dated.

What this report does not show

- Sources that were not connected, or tables the scan could not read (listed in section 3).
- Live activity. IRIS runs point-in-time scans that you schedule or run on demand.
- Fixes. IRIS flags and records; your teams make changes in the source system.
- A compliance opinion. This is evidence for your assessor, not a certification.

About this sample: produced from a real IRIS scan of a demo database containing synthetic records. Organization name and layout prepared by Sylox for illustration; values shown come from the scan results.