DutAIx
YOUR OWN LAB FOR AI REGULATION

ADVISORY REPORT · REQUIREMENTS PHASE

Credit card Application and Approval Project

A structured review of the submitted requirements, the duties the platform attaches, and what remains open before the requirements can be treated as complete.

PENDING OVERALL RESULT

4 Stories assessed	22 Duties applicable now	13 Story-level duties
9 Project-level duties	11 Future / readiness	16 Not applicable

Version 1 · 2026-11-10

Prepared by DutAIx · Advisory, not legal advice

What this assessment shows.

This report records the Requirements assessment for the credit-card application and approval project. It sets out what the submitted stories require, which duties the platform attaches, and what remains open before the requirements can be treated as complete.

PENDING

No story is recorded as Pass or Conflict. The four stories are all **Needs details**; the duty findings below explain what is missing.

Key findings

- The report records 4 submitted stories. All 4 are **Needs details**; no story is recorded as **Pass** or **Conflict**.
- The stories describe a straight-through credit-card decision, a short rejection reason, customer support and a view of submitted data. They do not specify a human review and contest route, a meaningful explanation, or access to the decision record.
- The platform attaches **DP-22-EU**, **DP-13** and **DP-17** to the story findings. It treats the missing explanation and challenge route as open requirements, not as completed controls.
- At project level, 9 duties are recorded as **Not met**, including DPIA, lawful basis, data protection by design, security, retention and risk-classification documentation.
- 11 high-risk AI Act duties are separated as **Future readiness** (from 2027-12-02). They are not counted as current findings.

SCOPE AND LIMITS

Only the Requirements module was run. Design, Build and QA were not run for this project.

The report is advisory, not legal advice. It is not a compliance certificate or an assurance that any incident would have been prevented. A qualified compliance team member should review the legal interpretation.

The legal basis is attached by the platform from the approved duty-to-law binding and knowledge base. Suggested acceptance scenarios are model-generated and unverified; they are for review, not legal requirements.

Detailed assessment

The full findings, duty tables, suggested details, annexure and audit trail from the saved Requirements run.

▾ User stories duties — findings and suggestions

Findings first; open suggested improvements when needed. Duty links show the assessment basis, including unresolved applicability.

▾ Needs details Story 1 — As an applicant, I want a straight-through decision on my credit-card application so that I get an answer immediately.

Duties directly engaged: **5** · Findings: **5**

Duty findings

DP-22-EU Needs details · Law: GDPR Art 22 shared · GDPR Art 13 shared

- A 'straight-through' accept/reject on a credit-card application is a solely automated decision with a significant effect on the applicant. The story is silent on how an applicant gets a person to review it, gives their view or contests it. If built with no such route, the decision would lack the required safeguards.

EU-AG-03 Needs details · Law: GDPR Art 22 shared

- A refusal is a high-impact action. The story does not say that rejections or disputed outcomes can be reviewed by a person, or that an applicant can ask for one.

DP-06 Needs details · Law: GDPR Art 6

- The story does not identify the lawful basis for the automated decision or for the income, employment, address and credit-history processing behind it. The basis, and whether it supports a solely automated decision, must be settled before building.

DP-35 Needs details · Law: GDPR Art 35

- Large-scale automated credit scoring of individuals is likely high-risk processing. The story gives no sign that a DPIA is completed and approved before go-live.

EU-DC-02 Needs details · Law: GDPR Art 13 shared

- The applicant is not told at collection that the decision is automated, nor given meaningful information about the logic and consequences.

▼ Suggestions on details that could improve the details (Model generated recommendation)

Model-written suggestion, not verified against the law. Review before use. · 5 acceptance scenarios

```
Scenario: Applicant can request human review of an automated decision
  Given An applicant has received an automated accept or reject outcome in the portal
  When The applicant selects 'Request human review' and submits a statement of their point of view
  Then A review case is created and assigned to a named human reviewer with authority to change the
outcome
  And The reviewer sees the applicant's statement and the data used
  And The applicant is told the review result and the reason in the portal
  And The request, statement and result are recorded against the application
```

```
Scenario: Rejections are contestable and reach a person
  Given The service has issued a rejection
  When The applicant contests the rejection or asks to speak to a person
  Then The case is queued for a human reviewer
  And No final adverse effect beyond the original refusal is applied until the review is completed
  And The applicant receives confirmation that a person is handling the case
```

```
Scenario: Lawful basis recorded for each purpose
  Given The processing purposes for the application and automated decision are listed
  When The privacy and legal owner reviews the design before build
  Then Each purpose names its lawful basis with reasoning
  And The record states which ground permits the solely automated decision and which safeguards apply
  And No purpose is left without a basis
```

```
Scenario: DPIA approved before go-live
  Given The release candidate for the automated decision service is ready
  When The go-live gate is evaluated
  Then An approved, dated DPIA covering the automated scoring and decision exists
  And The release is blocked if the DPIA is missing or does not cover the AI processing
```

```
Scenario: Applicant told the decision is automated before applying
  Given An applicant is about to submit the application form
  When The privacy notice is displayed at the point of data collection
  Then The notice states that the decision is made solely by automated means
  And It explains in plain words the main logic and the likely consequences
  And It states the right to human review and to contest
```

▾ Needs details **Story 2 — As an applicant, I want a short reason for rejection in the portal so that I can quickly understand the outcome.**

Duties directly engaged: **4** · Findings: **4**

Duty findings

DP-22-EU Needs details · Law: GDPR Art 22 shared · GDPR Art 13 shared

- A 'short reason' may be too thin for the applicant to understand the logic and to contest the decision, so it may not support a meaningful challenge.

DP-13 Needs details · Law: GDPR Art 13 shared · GDPR Art 14

- The story does not say the applicant gets meaningful information about the logic, significance and consequences of the automated decision, nor information on data obtained from credit-reference sources.

EU-DC-02 Needs details · Law: GDPR Art 13 shared

- The reason is shown in plain words but nothing links it to the automated decision logic or consequences, or to how to contest.

EU-AIA-50-P Needs details · Law: AI Act Art 50 shared

- If the rejection reason text is AI-generated, the applicant must be told they are dealing with an AI system and the text must carry a machine-readable marker. The story is silent on both.

▼ **Suggestions on details that could improve the details (Model generated recommendation)**

Model-written suggestion, not verified against the law. Review before use. · 4 acceptance scenarios

```
Scenario: Rejection reason enables contesting
  Given An application has been rejected by the automated service
  When The applicant opens the rejection in the portal
  Then The principal factors behind the rejection are shown in plain language, for example income,
credit history or employment data
  And A visible link or button lets the applicant request human review and contest the outcome
  And The factors shown match the factors the decision actually used
```

```
Scenario: Information on logic and data sources
  Given The decision used data from the applicant and from a credit-reference source
  When The applicant views the rejection reason or the linked privacy notice
  Then The notice names the categories of data used and the credit-reference source
  And It explains the significance and consequences of the automated decision
  And It lists the applicant's rights and how to exercise them
```

```
Scenario: Plain-word explanation of automated decision
  Given A rejected applicant views the outcome page
  When The page is rendered
  Then It states that the outcome was reached by automated processing
  And It explains the logic and consequences without technical jargon
  And A reviewer confirms the wording is understandable
```

```
Scenario: AI disclosure and marking of generated reason text
  Given The rejection reason is produced by a generative component
  When The reason is displayed to the applicant
  Then The applicant is told at first exposure that the text is AI-generated, unless this is obvious
from context
  And The output carries a machine-readable marker that a detection check finds on sampled outputs
```

▾ Needs details Story 3 — As an applicant, I want to contact customer support if I have a question about the decision so that they can explain it to me.

Duties directly engaged: **5** · Findings: **5**

Duty findings

DP-22-EU Needs details · Law: GDPR Art 22 shared · GDPR Art 13 shared

- Support is only framed as explaining the decision. Nothing lets the applicant obtain human intervention, put their view or contest the decision, so a question-only channel would not meet the required safeguards.

EU-AG-03 Needs details · Law: GDPR Art 22 shared

- The story does not say a request to speak to a person, or to contest a refusal, reaches a human who can act on it.

EU-HO-01 Needs details · Law: AI Act Art 14 shared

- Support staff who handle contested decisions need a way to override or reverse the automated outcome and to stop it, and that action must be logged. The story does not provide one.

EU-HO-02 Needs details · Law: AI Act Art 14 shared

- Support staff may simply defend the automated outcome. The story does not address over-reliance on the AI output.

EU-AIA-04 Needs details · Law: AI Act Art 4

- Support and review staff who explain and handle AI decisions need AI literacy training covering this system's limits.

▼ **Suggestions on details that could improve the details (Model generated recommendation)**

Model-written suggestion, not verified against the law. Review before use. · 5 acceptance scenarios

```
Scenario: Support contact leads to human review
  Given A rejected applicant contacts support about the decision
  When The applicant says they want the decision reviewed or contested
  Then Support opens a human review case with the applicant's statement
  And The applicant is told how long a response will take and the result is communicated
  And The case outcome is recorded
```

```
Scenario: Request to speak to a person
  Given The applicant uses the support channel, which may include an automated assistant
  When The applicant asks to speak to a person
  Then The request is handed to a human agent
  And The hand-over is confirmed to the applicant
```

```
Scenario: Reviewer can override and stop, with logging
  Given A human reviewer is handling a contested application
  When The reviewer overrides the automated outcome or halts the decision process
  Then The override or halt takes effect and the system stays in a safe state
  And The log records who acted, when and why
```

```
Scenario: Review screen avoids nudging blind acceptance
  Given A reviewer opens a contested case
  When The review screen is displayed
  Then It shows the main reasons and any confidence indicator for the automated outcome
  And No decision option is pre-selected
  And Reviewer guidance covering automation bias is available
```

```
Scenario: Support staff trained
  Given Staff will handle decision queries or reviews
  When Training records are audited before go-live
  Then Dated records show each such staff member trained on this system's limits, failure modes and
automation bias
```

▼ Needs details **Story 4 — As an applicant, I want to view the application information I submitted so that I can check it is complete and correct.**

Duties directly engaged: **3** · Findings: **3**

Duty findings

DP-17 Needs details · Law: GDPR Art 15 · GDPR Art 17

- Viewing submitted data supports access rights, but the story does not cover the other data the assessment used (for example credit-reference data) or exporting a copy. Correcting inaccurate data and erasing it are also not covered.

DP-32 Needs details · Law: GDPR Art 32 shared

- The portal exposes personal data, including income, employment and address. The story does not require authenticated, secure access or exclude personal data from logs.

DP-05 Needs details · Law: GDPR Art 5 shared

- The story does not say how long application data stays viewable or how long it is retained.

▼ **Suggestions on details that could improve the details (Model generated recommendation)**

Model-written suggestion, not verified against the law. Review before use. · 3 acceptance scenarios

```
Scenario: Applicant can view and obtain a copy of their data
  Given An authenticated applicant has submitted an application
  When The applicant opens 'My application' and requests a copy
  Then All submitted fields are shown
  And The data used in the decision, including external credit data, is accessible or obtainable on
request
  And A copy is provided in a commonly used electronic format
  And The applicant can flag inaccurate data for correction
```

```
Scenario: Application data only visible to the authenticated applicant
  Given A user is not authenticated or is a different applicant
  When They request another applicant's application view
  Then Access is denied
  And Data is encrypted in transit and at rest
  And Application logs contain no personal data fields
```

```
Scenario: Retention period for viewable application data
  Given The retention schedule is defined
  When The retention period for application data expires
  Then The data is deleted or anonymised by an automated job
  And The view no longer shows it
  And The schedule lists a purpose and a period for each data item
```

▾ Project-level duties — Findings and suggestions

Duties directly engaged: 9 · Findings: 9 · Not met: 9 · Met: 0 · Not assessable: 0

Duties applicable to the project as a whole, not linked to a submitted story. They are not demonstrated breaches.

Duty	Law	Status	Recommendation / Summary
DP-25 Data protection by design and by default	GDPR Art 25 shared	Not met	Keep personal data out of prompts/training where not needed; control what third-party models retain
EU-AG-01 Give an AI agent access only to the personal data each task needs (least privilege)	GDPR Art 25 shared	Not met	Separate credentials per agent; no shared admin keys

Duty	Law	Status	Recommendation / Summary
EU-AG-02 Secure the agent's identity, credentials and tool permissions	GDPR Art 32 shared	Not met	Secrets in a vault, never in code or prompts
EU-AG-04 Log what an AI agent does so its actions can be traced	AI Act Art 12 shared	Not met	Logs are tamper-evident and kept for the required period
EU-AIA-05 Screen out prohibited AI practices	AI Act Art 5 AI Act Art 5	Not met	No subliminal, manipulative or deceptive techniques that materially distort behaviour
EU-AIA-06 Document the risk classification	AI Act Art 6 AI Act Annex III AI Act Art 49 shared	Not met	Write the intended purpose precisely; classification follows it
EU-DC-01 Set and enforce retention periods for prompts, outputs, logs and training data	GDPR Art 5 shared	Not met	Retention set per data type; automatic deletion or anonymisation
EU-DC-05 Record the AI processing in the record of processing activities	GDPR Art 30	Not met	A user story or requirement that states the obligation and has acceptance criteria tied to this duty's provision.
EU-MO-01 Report personal-data breaches caused through the AI within 72 hours	GDPR Art 33	Not met	Monitoring that detects personal data in AI outputs

▾ Annexure

▾ Overview of duties with all stories

One row per story-level applicable duty. The **Stories** column lists the IDs linked to that duty; click an ID to expand the story. The current status is the duty's status; the recommendation says what is needed to resolve it. Pass duties have no recommendation.

Duty	Law	Stories	Current status	Recommendation
DP-05 Purpose limitation, data minimisation and storage limitation	GDPR Art 5 shared	R4	Needs details	Add: A stated purpose and retention period, with deletion on schedule.
DP-06 Lawful basis for processing	GDPR Art 6	R1	Needs details	Add: A documented lawful basis per purpose, including for the automated decision.

Duty	Law	Stories	Current status	Recommendation
DP-13 Information to people whose data is used	GDPR Art 13 shared GDPR Art 14	R2	Needs details	Add: Notice content covering these items, shown at or before collection.
DP-17 Access and erasure requests	GDPR Art 15 GDPR Art 17	R4	Needs details	Add: Access to all data used, export, correction and erasure across all stores.
DP-22-EU Safeguards for solely automated decisions (EU)	GDPR Art 22 shared GDPR Art 13 shared	R1 R2 R3	Needs details	Add: A tested route to request human review, express a view and contest, with a reviewer able to change the outcome.
DP-32 Security of processing	GDPR Art 32 shared	R4	Needs details	Add: Authentication, access control, encryption and no personal data in logs.
DP-35 Data protection impact assessment (DPIA)	GDPR Art 35	R1	Needs details	Add: A DPIA approved before go-live covering the AI processing.
EU-AG-03 Keep a human in the loop before an agent takes decisions with significant effects on people	GDPR Art 22 shared	R1 R3	Needs details	Add: Rejections can be queued for human handling, and a request to speak to a person reaches one.
EU-AIA-04 AI literacy of staff and operators	AI Act Art 4	R3	Needs details	Add: Dated training records for support and review staff.
EU-AIA-50-P Transparency duties of providers (AI interaction and content marking)	AI Act Art 50 shared	R2	Needs details	Add: Decide whether text is generated; if so, add disclosure and a machine-readable marker.
EU-DC-02 Tell people their data is used by AI, including any automated decisions	GDPR Art 13 shared	R1 R2	Needs details	Add: A plain-language notice at collection stating that the decision is automated, with the logic, consequences and rights.
EU-HO-01 Let overseers safely stop or override the system	AI Act Art 14 shared	R3	Needs details	Add: A logged override and stop path available to reviewers.
EU-HO-02 Help overseers avoid over-relying on the AI's output (automation bias)	AI Act Art 14 shared	R3	Needs details	Add: UI and guidance that avoid nudging blind acceptance.

▼ Future Readiness · 11

Duty ID	Duty	Law / reference	Applicability	Summary
EU-AIA-09	Risk management system	AI Act Art 9	Future / not in force today	Not in force today. Applies from 2027-12-02. Plan for: Eliminate or reduce risks by design before relying on warnings
EU-AIA-10	Data and data governance	AI Act Art 10	Future / not in force today	Not in force today. Applies from 2027-12-02. Plan for: Data relevant, sufficiently representative and as error-free and complete as possible for the purpose
EU-AIA-11	Technical documentation	AI Act Art 11 AI Act Annex IV	Future / not in force today	Not in force today. Applies from 2027-12-02. Plan for: Generate documentation from the pipeline (model cards, data cards, eval reports) to keep it current
EU-AIA-12	Automatic logging and log retention	AI Act Art 12 shared AI Act Art 19	Future / not in force today	Not in force today. Applies from 2027-12-02. Plan for: Log events that let you identify risk situations and substantial modifications, and support post-market monitoring
EU-AIA-13	Transparency to deployers (instructions for use)	AI Act Art 13	Future / not in force today	Not in force today. Applies from 2027-12-02. Plan for: Make outputs interpretable enough for deployers to use them appropriately
EU-AIA-14	Human oversight by design	AI Act Art 14 shared	Future / not in force today	Not in force today. Applies from 2027-12-02. Plan for: Reviewers can understand capabilities and limits, interpret output, disregard or reverse it, and stop the system
EU-AIA-15	Accuracy, robustness and cybersecurity	AI Act Art 15	Future / not in force today	Not in force today. Applies from 2027-12-02. Plan for: Resilience to errors, faults and inconsistencies; fail-safe fallbacks
EU-AIA-17	Quality management system	AI Act Art 17	Future / not in force today	Not in force today. Applies from 2027-12-02. Plan for: An ISO/IEC 42001 AI management system can provide much of this structure
EU-AIA-43	Conformity assessment, declaration, CE marking, registration	AI Act Art 49 shared AI Act Art 43 AI Act Art 47 AI Act Art 48	Future / not in force today	Not in force today. Applies from 2027-12-02. Plan for: Plan the conformity route early (internal control vs notified body)

Duty ID	Duty	Law / reference	Applicability	Summary
EU-AIA-72	Post-market monitoring plan	AI Act Art 72	Future / not in force today	Not in force today. Applies from 2027-12-02. Plan for: Build telemetry and feedback channels from deployers into the product
EU-AIA-73	Serious incident reporting	AI Act Art 73	Future / not in force today	Not in force today. Applies from 2027-12-02. Plan for: Detectability: alerts that surface potential serious incidents quickly

▼ Not applicable · 16

These duties are excluded in this project run. The law/reference is the catalogue source and provision; the duty was not assessed.

Duty	Law / reference	Summary
EU-AIA-26 Deployer duties for high-risk AI	AI Act Art 26	Not applicable in this run: The project is a provider; this duty applies to deployers.
EU-AIA-27 Fundamental rights impact assessment (FRIA)	AI Act Art 27	Not applicable in this run: The project is a provider; this duty applies to deployers.
EU-AIA-86 Explanation of individual decisions	AI Act Art 86	Not applicable in this run: The project is a provider; this duty applies to deployers.
EU-AIA-50-D Transparency duties of deployers (emotion recognition, deepfakes, public-interest text)	AI Act Art 50 shared	Not applicable in this run: The project is a provider; this duty applies to deployers.
EU-AIA-53 General-purpose AI model provider duties	AI Act Art 53 AI Act Annex XI AI Act Annex XII	Not applicable in this run: The project does not train or place a general-purpose AI model on the market.
DP-09 Condition for special-category data	GDPR Art 9	Not applicable in this run: The project does not use special-category personal data.
DP-44 Transfers of personal data outside the EU	GDPR Art 44 GDPR Art 45 GDPR Art 46 GDPR Art 49	Not applicable in this run: Personal data does not leave the UK/EU.
EU-DC-03 Have a processor contract with the AI model or API vendor	GDPR Art 28	Not applicable in this run: The project does not meet this duty's condition (external_model_vendor: needs yes, project has no).
EU-DC-04 Put safeguards in place when personal data goes to a model hosted in another country	GDPR Art 44	Not applicable in this run: Personal data does not leave the UK/EU.

Duty	Law / reference	Summary
EU-IM-01 Importer: verify the provider's conformity before placing a high-risk AI system on the EU market	AI Act Art 23	Not applicable in this run: The project is a provider; this duty applies to importers.
EU-IM-02 Importer: hold back a system that may not conform, and inform the provider and authorities of risks	AI Act Art 23	Not applicable in this run: The project is a provider; this duty applies to importers.
EU-IM-03 Importer: show the importer's name and contact address on the system or its documentation	AI Act Art 23	Not applicable in this run: The project is a provider; this duty applies to importers.
EU-IM-04 Importer: keep the certificate, instructions for use and EU declaration for 10 years	AI Act Art 23	Not applicable in this run: The project is a provider; this duty applies to importers.
EU-DI-01 Distributor: verify CE marking, EU declaration and instructions for use before making the system available	AI Act Art 24	Not applicable in this run: The project is a provider; this duty applies to distributors.
EU-DI-02 Distributor: do not make a non-conforming system available; correct, withdraw or recall it and inform others	AI Act Art 24	Not applicable in this run: The project is a provider; this duty applies to distributors.
EU-VC-01 If you put your name on it, change it substantially or change its purpose, you take on the provider's duties	AI Act Art 25	Not applicable in this run: The project is a provider; this duty applies to deployers, importers or distributors.

2 duties from other jurisdictions are not reported in this project report.

▼ Audit trail: recorded assessment and evidence

The technical record behind this report: each duty, criterion, evidence examined, mapping state and outcome, plus model, catalogue and law provenance. The report's findings are generated from this same saved run.

The recorded assessment and technical evidence are retained in the platform.

> This is an advisory tool, not legal advice. This is an AI-assisted report. We advise that a qualified compliance team member should review the legal interpretations. The legal basis shown for each duty is attached by the platform from the approved duty-to-law binding and knowledge base.