

SPR MARKET-SOUNDING PACKAGE

Annex A

SPR Portal

High-Level, Outcome-Based Requirements

Technology-neutral market sounding | Non-binding | Vendor solution approach requested

Document field	Value
Version	2.0
Related document	SPR Market-Sounding Master Document
Module	SPR Portal
Purpose	Indicative vendor feasibility, approach, effort, timeline and cost assessment

How to read this annex / This annex defines required business outcomes and non-negotiable boundaries. It does not prescribe screen layouts, detailed forms, exact workflow steps, status catalogues, API schemas or technical products. Vendors are expected to propose a coherent implementation approach and clearly state assumptions, dependencies and alternatives.

Contents

1. Purpose and document status
2. Business objective
3. Scope and boundaries
4. Users and required outcomes
5. High-level capability areas
6. Logical context and processing outcomes
7. Shared requirements
8. Integrations and dependencies
9. Sizing and assumptions
10. Preliminary MVP and full implementation
11. Design-stage decisions
12. Vendor response requirements

1. Purpose and document status

This annex describes the required outcomes for a subject-facing digital Portal through which SPR Subjects can access approved State Population Register (SPR) services, submit applications or permitted updates, provide evidence, respond to requests and understand the status and outcome of their actions. It supports market sounding and is not a final solution design or procurement specification.

- Technology-neutral. No low-code platform, product or architecture is mandatory for this annex.
- Self-contained. Vendors should be able to prepare an indicative response without receiving internal source documents.
- Outcome-based. The annex defines what the Portal must achieve and the boundaries it must respect.
- Non-binding. The market-sounding exercise does not constitute a tender or commitment to procure.

2. Business objective

The objective is to provide SPR Subjects with a secure, understandable and traceable action channel for approved SPR-related services, while preserving the role of MyData as a data-viewing and possible entry channel, the role of CMS / Back Office for case-based processing, and the authority of SPR Core for final registration and authoritative data updates.

Core business outcome / An SPR Subject can start an approved action, provide the required information or evidence, follow progress, respond to requests and receive a clear result - without the Portal directly editing the SPR database or exposing internal government processing information.

3. Scope and boundaries

3.1 Mandatory baseline scope

- Secure access through direct Portal access and other approved entry or redirect channels.
- Initiation and submission of approved correction, update or completion applications.
- Support for permitted direct updates where legal and business rules allow them.
- Evidence upload or reference through the shared Evidence Document Management Service.
- Subject-facing application status, pending actions, decisions/results and relevant history.
- Response to requests for additional information or evidence.
- Subject-facing notifications and approved communication preferences.
- Integration with CMS / Back Office, SPR Core or approved data services, IAM/SSO, notifications, evidence services and approved entry channels.
- Audit, monitoring, administrative configuration and supportability.

3.2 Separately priced optional scope

- Authorized Representative functionality, including representation-basis validation where required.
- Document or certificate issuance requests and related Portal presentation.
- OCR or automatic extraction from uploaded evidence documents.
- Other optional functionality clearly identified by the vendor and excluded from baseline totals.

3.3 Out of scope

- Replacement of MyData as the general SPR Subject data-viewing platform.
- Direct editing of the SPR database or bypass of SPR Core validation and authoritative update rules.
- Creation, selection or modification of a PSN outside SPR Core.
- Display of internal case notes, restricted government communication or internal audit logs.
- Unrestricted access to another person's data or applications.
- Data-provider-body operational functionality, which is covered by the separate provider annex.
- Construction of external IAM, MyData, notification, address or other government systems.
- A native mobile application unless separately requested and priced.

4. Users and required outcomes

User / channel	Required outcome
SPR Subject	Access approved services for their own permitted context; submit data/evidence; follow status; respond to requests; receive understandable outcomes.
Authorized Representative - optional	Act within a verified representation scope where the optional module is ordered and the legal basis is confirmed.
Approved entry channel	Redirect or deep-link the subject to the appropriate Portal context without exposing sensitive data or replacing the Portal.
Portal content / service administrator	Maintain approved service descriptions, guidance, templates and configurations without unrestricted access to subject data.
Support function	Use non-sensitive references and approved support information to assist users without accessing more personal data than necessary.

5. High-level capability areas

Capability area	Required business outcome
Access and service entry	Authenticate the subject through approved mechanisms and present only the services and actions available in the permitted context.
Applications and updates	Allow the subject to prepare and submit approved applications or permitted updates with clear guidance and confirmation.
Permitted direct changes	Process only data fields explicitly approved for direct update; route conflicts or failed validations to an appropriate exception path.
Evidence and responses	Allow required evidence and additional-information responses to be provided through the shared document capability.
Status and communication	Provide a simple subject-facing view of progress, required actions, decisions/results and approved notifications.
History and transparency	Provide an appropriate subject-visible history without exposing internal workflow, restricted reasons or internal government communications.
User assistance and accessibility	Provide understandable guidance, validation messages and an inclusive responsive web experience.
Administration and configuration	Support controlled configuration of services, content, rules, templates, visibility and other approved parameters.

Not prescribed at market-sounding stage / Exact screens, navigation, information architecture, form layouts, field catalogues, detailed validation rules, status lists, content-management products and technical architecture are not fixed by this annex. Vendors should propose a practical and maintainable approach.

6. Logical context and processing outcomes

The Portal is the subject-facing action layer of the integrated solution. It may be reached directly or through approved entry channels such as MyData or eGov. The diagram below is illustrative and does not prescribe a final deployment or component architecture.

SPR Portal – Preliminary Logical Context

State Population Register (SPR) – Market Sounding

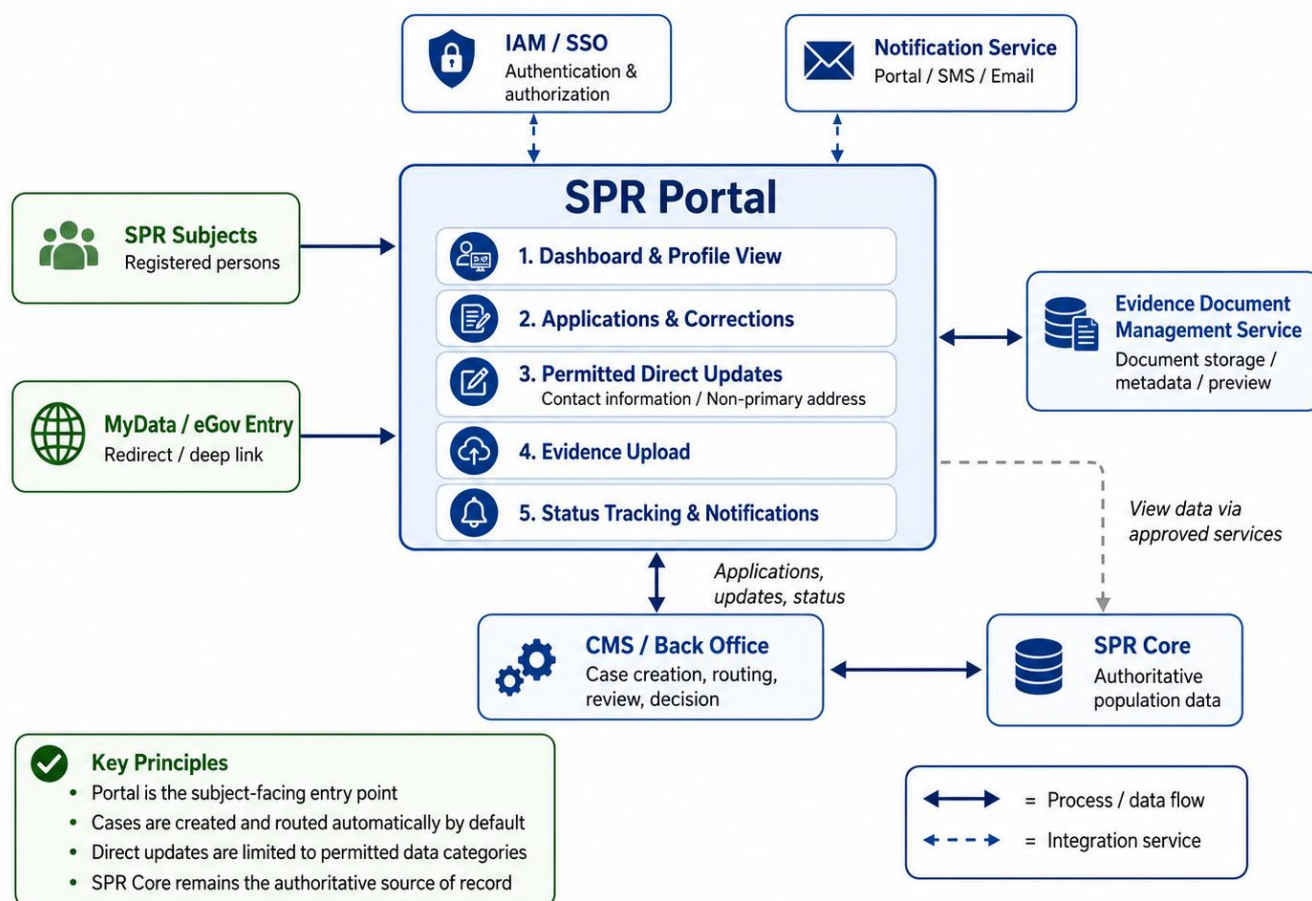


Figure 1. Preliminary logical context. The Portal supports case-based actions, permitted direct updates and shared-service integrations while SPR Core remains authoritative.

6.1 Non-negotiable principles

- MyData may remain a data-viewing platform and an entry channel; the Portal must also be accessible through other approved channels.
- SPR Core remains the authoritative source and performs final registration and authoritative data updates.
- The Portal must not directly edit the SPR database or generate a PSN.
- Case-based submissions should create and route the relevant CMS case automatically by default.
- Direct updates are permitted only for approved data categories and successful validations.
- Internal, restricted or non-subject-facing information must not be exposed through the Portal.
- Material user, data, evidence, status and security actions must be traceable.

6.2 High-level processing outcomes

Processing pattern	High-level outcome
Case-based application	The subject submits an approved application; CMS creates and routes a case, manages review/decision, and returns a subject-facing status and result.
Permitted direct update	The Portal submits an approved data change through an authorized service; success is confirmed, while a conflict or failed validation follows an approved exception path.
Additional information / evidence	The subject receives a clear request, provides the required response or evidence, and the connected case continues with full traceability.
Approved entry / redirect	MyData, eGov or another approved channel transfers a valid service context to the Portal without exposing sensitive data in the URL or bypassing authentication.
Evidence handling	The Portal uses the shared evidence service for upload, preview/reference and access control; actual files are not stored in SPR Core.
Notification and result	The subject receives an approved Portal, SMS, email or other notification and can view the relevant subject-facing outcome in the Portal.

7. Shared requirements

Area	High-level expectation
Security and privacy	Strong identity, session and access controls; own-data access; data minimization; protection of personal and restricted information.
Audit and accountability	Traceable actor, action, object, time and outcome for significant submissions, updates, evidence actions, communication and security events.
Usability and accessibility	Understandable language, practical guidance, responsive web design and an accessibility approach proposed by the vendor.
Configurability	Service catalogue, content, forms, visibility, status mapping, notification templates and permitted actions should be configurable where appropriate.
Reliability and recoverability	Safe handling of expired links, failed integrations, interrupted submissions, duplicate actions and service unavailability.
Maintainability	Reusable components, documented interfaces, controlled releases and minimal dependency on undocumented custom logic.
Observability	Monitoring of user-impacting errors, integration failures, evidence/notification issues, performance and security events.
Privacy by design	Only necessary data should be displayed or collected; masking and disclosure restrictions must be supported where required.

8. Integrations and dependencies

System / service	Purpose and boundary
IAM / SSO	Authentication, identity verification, authorization, session and logout. Final protocols and identity-matching rules are design-stage decisions.
MyData / eGov / approved entry	Redirect or deep-link context. These are entry/viewing channels and are not replaced by the Portal.
CMS / Back Office	Automatic case creation, subject-facing status, requests, decisions and results for case-based actions.
SPR Core / approved data services	Permitted direct updates, authoritative outcomes and person/data references. No direct database access.
Evidence Document Management Service	Upload, metadata, secure preview/reference, visibility, linkage and audit. Actual files remain outside SPR Core.
Notification service	Portal, SMS, email or other approved channels; delivery status and failure handling.
Address / Cadastre services	Approved address search or validation where applicable; exact services and primary-address process remain to be confirmed.
Audit / monitoring platform	Security, operational and material business events in the target government environment.

Integration detail / Detailed endpoint catalogues, payloads, error codes, event/callback patterns, credentials, retry rules and service ownership are design-stage decisions. Vendors must state assumptions and include reasonable interface-definition effort.

9. Sizing and assumptions

Parameter	Current market-sounding baseline
Registered persons	300,000+.
Back Office users	1,000+.
Provider organizations	10-30.
Concurrent users	200 overall solution baseline.
Cases / transactions	100,000+ cases per year overall solution baseline.
Growth	Vendor should explain scaling approach and principal capacity drivers.

10. Preliminary MVP and full implementation

10.1 Preliminary MVP

The vendor should propose a practical MVP that demonstrates end-to-end subject access and action while preserving the non-negotiable boundaries in this annex. The proposed MVP should cover, at minimum:

- secure direct access and at least one approved redirect/entry pattern;
- subject authentication and access to permitted services;
- a representative correction/update application that automatically creates and routes a CMS case;
- a representative permitted direct update, subject to approved rules;
- evidence upload/reference and response to an additional-information request;
- subject-facing status, notifications and relevant history;
- audit, basic administration and operational monitoring.

10.2 Full implementation

The full implementation should support the approved Portal service catalogue, final business and legal rules, agreed integrations, configured status and notification models, user assistance, localization/accessibility, operational monitoring and scalable support for the confirmed programme baseline.

11. Design-stage decisions

The following details are intentionally not finalized for market sounding. The required capability is part of the baseline; the exact configuration will be confirmed during analysis and design.

Decision area	To be confirmed
Final Portal service catalogue	Priority services, application types, MVP sequencing and ownership.
Portal versus MyData display	Exact data displayed in the Portal for each action and the return/continuation experience.
Permitted direct-update catalogue	Data fields, validations, consent/verification and exception-routing rules.
Primary-address process	Actors, evidence, ownership, approvals and whether it is included in the initial release.
Subject-facing statuses and results	Terminology, mapping, permitted history and decision/rejection disclosure.
Entry and redirect rules	Approved channels, token/context model, deep links, expiry and return behavior.
Notifications	Channels, priority, preferences, retry/failure behavior and content ownership.
Evidence behavior	Document requirements, visibility, secure preview/download and draft/retention rules.
Language and accessibility	Additional languages, translation ownership, accessibility standard and browser matrix.
Authorized Representative option	Representation types, legal basis, verification and permitted scope if ordered.
Detailed integration contracts	APIs/events, error models, correlation, retry/idempotency and service ownership.
Portal-specific sizing	Active users, peak sessions, submission volumes, documents and notifications.

12. Vendor response requirements

The vendor response should be concise but sufficiently detailed to support market comparison. Vendors should provide:

Response area	Requested information
Understanding of need	Summary of the subject-facing problem, intended outcomes and important programme boundaries.
Proposed solution approach	High-level Portal architecture, major components, configuration approach and technology choices.
User experience approach	Service entry, navigation, form strategy, plain-language guidance, responsive design and accessibility assumptions.
Processing approach	Case-based submissions, permitted direct updates, evidence responses, status and notifications.
Integration approach	IAM/SSO, MyData/eGov, CMS, SPR Core/approved data services, evidence, notifications, address and monitoring assumptions.
Security and privacy	Own-data access, session/redirect security, data minimization, disclosure control, audit and evidence access.
Sizing and performance	Capacity model using the confirmed baseline and justified assumptions for unknown Portal peaks.
MVP proposal	Recommended scope, sequencing, calendar duration, person-days, team and total price in AMD with VAT treatment.
Full implementation	Calendar duration, person-days, team composition and total price in AMD with VAT treatment.
Optional scope	Separate effort, duration and price for Authorized Representative, document issuance and OCR/automatic extraction.
Warranty and support	Separate 12-month service description and price, including incident and maintenance assumptions.
Risks and dependencies	Key Customer, Core, CMS, infrastructure, legal, content and decision dependencies; risks and mitigation.
Deviations and alternatives	Any unsupported requirement, proposed alternative, exclusion or condition affecting price or timeline.

Market-sounding principle / Vendors are not expected to reproduce a predefined Portal solution. They are expected to demonstrate that their proposed approach can achieve the required subject outcomes, respect programme boundaries and provide credible assumptions, effort and cost information.

End of Annex A