RULES AND TECHNICAL GUIDELINES

Table of Contents

DJANTA CHALLENGES 2026 COMPETITION RULES

PREAMBLE

As part of the implementation of the Togo Digital National Strategy and the promotion of technological innovation in Togo, the Djanta Tech Hub organizes challenges for the ecosystem.

This national competition comprises two distinct and complementary programs:

- Djanta Innova – Innovation Challenge
- Djanta Idea-Action – Hackathon

The challenges aim to identify, promote and support innovative solutions that address national development priorities in strategic sectors.

ARTICLE 1: OBJECTIVES OF THE COMPETITION

The challenges pursue the following objectives:

1. Identify innovative solutions with a strong economic and social impact in priority sectors;
2. Supporting selected teams in structuring, developing and bringing viable products or services to market;
3. To contribute to strengthening and structuring the national ecosystem of innovation and technological entrepreneurship.

ARTICLE 2: PROGRAMS AND ELIGIBILITY REQUIREMENTS

The two programs focus in particular on the following sectors, without this list being exhaustive: Agriculture, Education, Crafts, Tourism, Finance, Logistics, SME Productivity, Optimization of public services and other national priorities.

2.1 Djanta Innova (Innovation Challenge)

The program is open to startups, small and medium-sized enterprises (SMEs), social enterprises, individual entrepreneurs, researchers, academics, professionals, and non-governmental organizations (NGOs).

Submitted projects must have reached a sufficient level of maturity and have, at a minimum, a functional prototype, a minimum viable product (MVP) or a technically demonstrable solution.

2.2 Djanta Idea-Action (Hackathon)

The program is aimed at students, recent graduates, and young professionals at the beginning of their careers.

The expected projects should be at the ideation stage, whether it is a pre-ideation phase or an initial idea, without a prototype or a minimum viable product (MVP) being required at this stage.

ARTICLE 3: CONDITIONS OF PARTICIPATION

3.1 General Eligibility

Each candidate or team may only submit one application and to one program.

All team members must be Togolese citizens or legal residents of Togo.

Applications can be submitted in French or English. Communications and presentations during bootcamps can also be given in French or English.

Teams consist of two (2) to five (5) members. Individual applications are accepted for the " Djanta Innova" program, although collaboration is strongly encouraged.

The participation of inclusive teams (gender, region, people living with disabilities) is strongly encouraged.

3.2 Participant Engagement

All candidates agree to abide by the competition's code of conduct, which is based on collaboration, mutual respect, ethics, and the originality of projects.

Selected participants commit to taking part in all activities of the selected program (bootcamps , workshops, mentoring sessions, final events);

3.3 Originality of projects and solutions

Submitted projects must be original and not infringe on any third-party intellectual property rights.

Participants retain full ownership of their ideas, projects and solutions.

However, participants authorize the Djanta Tech Hub to use project information for communication, promotion and institutional reporting purposes.

3.4 Grounds for disqualification

Any application may be disqualified in the event of:

- providing false or misleading information;
- plagiarism or fraudulent appropriation of existing concepts;
- failure to comply with deadlines, competition rules or participation commitments.

ARTICLE 4: APPLICATION FILE

4.1 File Contents

Program	Required elements
Djanta Innova	• Completed online form • Solution description (maximum 300 words) • Pitch deck • user interface demonstration or design (for MVP) • Team presentation • CV or LinkedIn profile of the team leader (optional)
Djanta Idea-Action	• Application form with information about the team • Summary of the initial idea (maximum 500 words) • Team member biographies • CV or LinkedIn profile of the team leader (optional)

4.2 Submission Procedures

Applications are submitted exclusively via the official platform through the link provided on the website.

ARTICLE 5: COMPETITION CALENDAR

The competition schedule unfolds according to these stages:

- Applications open: February 27, 2026
- Application deadline: April 10, 2026
- Pre-selection phase: April 10-18, 2026
- Bootcamps and coaching sessions: April 27 and 28, 2026
- Final pitch day: April 30, 2026
- Final selection: May 1, 2026

ARTICLE 6: JURY SELECTION PROCESS

The projects are evaluated by an independent jury based on the following criteria:

1. Relevance and alignment with national priorities;
2. Innovative and creative nature of the solution;
3. Potential for economic and social impact;
4. Quality, complementarity and commitment of the team;
5. Technical feasibility and viability of the project.

ARTICLE 7: PRICES AND OPPORTUNITIES

7.1 Djanta Innova – Winning Projects

The selected teams will notably benefit from:

- access to the Djanta Innovation Challenge Bootcamp ;
- participation in the final pitch day;
- integration into the Djanta Tech Hub incubation program ;
- support including mentoring, technical assistance, access to coworking and funding opportunities;
- visibility among investors and partners.

7.2 Djanta Idea-Action – Best Teams

The selected teams will notably benefit from:

- participation in a Sprint and Bootcamp Hackathon;
- Final Pitch Day ;
- access to a pre-incubation program ;
- support in designing MVPs, mentoring, access to coworking spaces and funding opportunities;
- visibility .

ARTICLE 8: INTELLECTUAL PROPERTY

Participants retain full intellectual property rights to their projects.
The Djanta Tech Hub is authorized to use their work for communication, promotion, and reporting purposes .

ARTICLE 9: DATA PROTECTION

In accordance with the provisions of Law No. 2019-014 of October 29, 2019 relating to the protection of personal data, participants consent only, on the relevant legal bases, to the use of their personal data in the context of communications relating to the Djanta challenges .

ARTICLE 10: COMPLAINTS

Claims relating to any problem or event related to the challenges are only admissible within a maximum period of fifteen (15) calendar days from the proclamation of the results.

ARTICLE 11: ACCEPTANCE OF THE REGULATIONS

Submitting an application constitutes full and unreserved acceptance of these regulations. All participants agree to abide by all of its provisions.

TG

TECHNICAL GUIDELINES

Djanta Tech Hub Challenge

Relevant Challenge Sector: Public Service

Preamble

These guidelines are intended for all teams participating in the application and digital integration development challenge organized as part of the launch of the Djanta Tech Hub. They constitute a mandatory framework aimed at ensuring that the solutions produced are reusable, sovereign, interoperable, and sustainable within the Togolese national digital ecosystem.

These rules apply regardless of the nature of the contribution: developing a solution from scratch, configuring an existing tool, integrating several software components, or adapting an open-source solution. They should not be applied dogmatically, but constitute a formal framework for work, a guiding principle that each team commits to respecting in both spirit and letter.

GUIDELINE 1 — Open Source & Open Standards

> **Rule:** Any submitted solution must be based on open source components and be published under a recognized open source license (MIT, Apache 2.0, GPL v3 or EUPL).

The use of open-source technologies is a non-negotiable condition for any solution intended for the Togolese public administration. This guarantees that the State retains ownership of its tools, can freely audit them, develop them further, and entrust them to other teams without being dependent on a single vendor. A proprietary licensed solution cannot be considered a digital public good.

The data formats, exchange protocols and exposed interfaces must also be based on open and documented standards, accessible to any player in the ecosystem without technical or commercial barriers.

What this means in practical terms:

- The source code or complete configuration files must be hosted on a public repository (GitHub, GitLab , Gitea , etc.) upon submission.
- The data formats used (exchanges, exports, storage) must be open formats: JSON, XML, CSV, PDF/A, ODF — never proprietary locked formats.
- API protocols must comply with open standards: REST/JSON, GraphQL , OpenAPI 3.x.
- No dependency on a non-substitutable proprietary component is permitted.

Premise Deployment & Infrastructure Independence

> **Rule:** The solution must be able to be deployed and operated entirely on a national infrastructure, without mandatory dependence on an external third-party cloud service.

Public digital solutions cannot rely on infrastructures whose continuity, confidentiality, and location are beyond the control of the State. Therefore, any submitted solution must be configured and delivered in such a way as to operate autonomously on available national infrastructures, whether physical servers, a government data center, or a regional sovereign cloud.

If external services are used as an option, they must be clearly identified and have a documented local alternative. The portability of the solution is a fundamental evaluation criterion.

What this means in practical terms:

- The solution must be containerized (Docker / Docker Compose required) to allow reproducible deployment on any infrastructure.
- It should not require connection to external cloud services to function (no mandatory dependency on AWS S3, Google Firebase , Azure AD, etc.).
- If external services are used, they must be replaceable and documented as such (e.g., MinIO storage as a local replacement for S3).
- A docker- compose.yml file allowing the entire solution to be launched with a single command is required.
- The solution must work in a low bandwidth environment if it is intended for field use.

GUIDELINE 3 — Interoperability & Integration into the National Ecosystem

> **Rule:** The solution must be configured and delivered in such a way as to integrate into the national digital ecosystem (Xportal , Xflow , national identification systems, etc.).

An isolated solution, however technically excellent, has no value in a public ecosystem if it cannot communicate with other government systems. Interoperability is not an optional feature—it is a structural requirement. Each solution selected for this challenge must be conceived as a component of a larger ecosystem, capable of exchanging data and delegating or consuming shared services.

This requirement applies to both technical interfaces (APIs) and data models, which must align with national standards where they exist.

What this means in practical terms:

- Exposure or activation of a REST API documented in OpenAPI /Swagger format.
- OAuth 2.0 / OpenID authentication protocol Connect to integrate with the national identity system.
- Every business entity exchanged (citizen, act, request, payment) must reference a standardized national identifier if available.
- A data dictionary describing all fields exposed by the API must be provided.
- Notifications must be able to be routed to national channels (SMS, email, push notification) via standardized interfaces.

GUIDELINE 4 — Modular & Replicable Architecture

> **Rule:** The solution must be based on a modular architecture allowing its reuse, adaptation and application to other administrative contexts or other scales.

Public investment in digital technology only makes sense if it can be leveraged and scaled. A solution implemented for one ministry must be adaptable and deployable in another context without starting from scratch. This implies a clear separation of responsibilities within the architecture, outsourced configuration, and documentation that allows a third-party team to understand, adapt, and extend the solution.

Modularity is also a guarantee of scalability: a well-structured architecture allows for the integration of new modules or the replacement of components without destabilizing the entire system.

What this means in practical terms:

- Clear separation of frontend / backend / database with defined contractual interfaces.
- The business modules must be independent and replaceable without a complete overhaul.
- The configuration (environment, URLs, keys) must be externalized via environment variables (.env file), never hard-coded.
- The solution must include an adaptation guide explaining how to deploy it for another service or administration.
- Generic components (authentication, notifications, audit log) must be usable as reusable building blocks.

GUIDELINE 5 — Safety by Design

> **Rule:** Security must be integrated from the outset, during the selection and implementation of the solution, and not addressed as an afterthought.

Digital public systems are prime targets. A vulnerability in a solution can compromise the data of thousands of citizens, disrupt public services, and erode trust in the state. Therefore, security cannot be treated as a late addition or a superficial layer; it must be a central concern from the very first configuration and architectural decisions.

Each team is responsible for integrating good security practices at all stages of the solution implementation, from database configuration to user session management, including communications protection and logging of sensitive actions.

What this means in practical terms:

- Strong authentication is mandatory for any access to personal or sensitive data (at least signed JWT, ideally OAuth 2.0).
- Encryption of sensitive data in transit (HTTPS/TLS 1.2+) and at rest.
- No sensitive data (passwords, API keys, credentials) in the source code or Git repositories.
- **Enabling basic OWASP protections:** protection against SQL injection, XSS, CSRF, etc.
- Logging of all sensitive actions with timestamps — logs must be viewable and unmodifiable.
- A simplified backup and recovery plan must be documented.

GUIDELINE 6 — Transparency, Traceability & Accountability

> **Rule:** All significant actions in the system must be traceable, auditable, and understandable by the relevant stakeholders.

Citizens' trust in digital public services largely depends on their ability to understand what is done with their data and to verify that the processes are fair and honest. This implies that all automated decisions must be explainable, that all processing of personal data must be justified and documented, and that administrators must have the necessary tools to exercise effective oversight of the system.

Traceability is not just a regulatory requirement — it is an essential governance mechanism for the responsible management of a public service.

What this means in practical terms:

- Enabling an audit log for critical operations: creation, modification, deletion of data, connections.
- Automatic decision algorithms (if applicable) must be explainable and documented.
- The personal data collected must be listed, justified and protected in accordance with the principles of data minimization.
- The solution must allow an administrator to view the history of actions without the possibility of altering the logs.
- Clear user documentation should explain how the data is used.

GUIDELINE 7 — Documentation & Skills Transfer

> **Rule:** The solution must be sufficiently documented so that a Togolese team can maintain, develop and manage it autonomously, without external assistance.

The sustainability of a public digital solution depends not only on its initial technical quality—it depends on the ability of national teams to ensure its continuity over time. An undocumented solution is a fragile one, whose long-term viability hinges on the availability of its original designers or integrators. Documentation is therefore a deliverable in its own right, just like the code or configuration files.

This requirement for skills transfer is also a concrete way to contribute to strengthening the Togolese digital ecosystem in the long term.

What this means in practical terms:

The submission must include the following documents:

Document	Expected content
README.md	Overview, prerequisites, quick installation
Installation Guide	Complete step-by-step deployment or configuration
User guide	Manual for agents and/or citizens
API documentation	OpenAPI (Swagger) specification of all exposed endpoints
Contribution Guide	How to modify, configure or contribute to the solution

- The code or configuration files must be commented in the complex parts, in French or English.
- Validation tests must be included to attest to the proper functioning of the solution (minimum recommended coverage: 60% for developed solutions).

GUIDELINE 8 — Creating Measurable Public Value

> **Rule:** Each solution must clearly demonstrate the value it brings to citizens or the administration, with measurable indicators.

A digital initiative in the public sector is only legitimate if it produces a real and verifiable impact on the quality of service provided or on the efficiency of administrative processes. It is not enough for a solution to be technically sound: it must address a documented need, target an identified beneficiary population, and define from the outset the indicators that will allow its success to be evaluated.

This focus on public value is what distinguishes a government innovation project from a mere technical exercise.

What this means in practical terms:

- **The submission must include a concrete use case:** problem solved, target beneficiary, expected impact.

- **Key performance indicators (KPIs) must be defined:** number of users, reduction in processing time, decreased error rate, savings generated, etc.
- The solution must address a documented need of the Togolese administration or citizens.
- A basic monitoring dashboard must be integrated or clearly planned in the roadmap.

TECHNICAL GUIDELINES

Djanta Tech Hub Challenge

Sectors covered by the Challenge : Agriculture, Education, Finance, Tourism and Culture, Trade and Crafts, Logistics, Creative Industries, SME Productivity

Preamble

These guidelines are for teams participating in the Djanta Tech Hub challenge whose solution is intended for the private market: startups, consumer applications, B2B tools, sectoral platforms, or any other digital product that meets a need of the Togolese market or the sub-region without necessarily interacting with the public administration.

These guidelines provide a framework, not a rigid set of specifications. Each team is encouraged to use them as inspiration, depending on the nature and maturity of its solution. The more a solution aligns with these best practices, the more robust, maintainable, adoptable, and likely to evolve favorably within the regional digital ecosystem.

GUIDELINE 1 — Open Standards & Technical Interoperability

> **Recommendation:** It is recommended that the solution rely on open technical standards for its data formats, exchange protocols and interfaces, in order to promote interoperability and avoid closed technical dependencies.

A private solution is not necessarily intended to publish its source code, and that is not what is expected here. However, the choice of formats and technical protocols has a direct impact on the solution's ability to integrate with other tools, to be adopted by partners, and to evolve over time without being locked into a proprietary technology.

Relying on open standards is a strategic choice as much as a technical one: it reduces integration costs, expands the pool of developers capable of contributing to the project, and facilitates future business partnerships.

Associated best practices:

- Prefer open data formats for exchanges and exports: JSON, XML, CSV, PDF/A.
- **Exposing APIs based on recognized standards:** REST/JSON, GraphQL , OpenAPI 3.x.

- Avoid proprietary formats or protocols that would make the solution difficult for third parties to integrate.
- If part of the code is generic and reusable, consider publishing it as open source to benefit from community contributions.

GUIDELINE 2 — Portability & Avoidance of Vendor Lock-in

> **Recommendation:** It is recommended to design the solution in such a way as not to create irreversible dependencies on a single cloud service or infrastructure provider.

Using cloud services is perfectly legitimate for a private solution, and often even recommended to accelerate development and reduce initial operating costs. The risk to anticipate is vendor lock-in: excessive dependence on a single provider can ultimately constrain technical choices, increase costs unexpectedly, or weaken the solution in the event of changing commercial conditions.

The goal is not to avoid the cloud, but to maintain strategic flexibility. A portable solution is one that retains control over its options.

Associated best practices:

- Abstracting dependencies on cloud services (storage, messaging, authentication) behind replaceable interfaces.
- Favor services with open source or multi-vendor alternatives (e.g., S3-compatible, standard SMTP, standard OAuth).
- Consider containerization (Docker / Docker Compose) to facilitate portability between environments.
- Document external dependencies and their potential alternatives.

GUIDELINE 3 — Interoperability & Openness to the Ecosystem

> **Recommendation:** It is recommended that the solution expose interfaces allowing its integration with other tools and services, in order to be part of an open digital ecosystem rather than operating in silos.

A solution that integrates easily with other tools has a real competitive advantage: it can be adopted more quickly, incorporated into existing workflows, and recommended by partners. Conversely, a closed solution creates friction for adoption and limits its market reach.

Interoperability is also a factor in scalability: it allows certain functions to be delegated to specialized services (payment, identity, notification) rather than rebuilding everything, which accelerates development and reduces technical debt.

Associated best practices:

- Expose a documented API in OpenAPI /Swagger format to facilitate integration by partners or third parties.
- Provide webhooks or event mechanisms to allow other systems to react to the actions of the solution.
- Rely on recognized authentication standards (OAuth 2.0, OpenID) Connect) to facilitate SSO integrations.
- Provide a data dictionary or documentation of the exposed models.
- Provide connectors or integration guides with the most commonly used tools in the target sector.

GUIDELINE 4 — Modular & Scalable Architecture

> **Recommendation:** It is recommended to adopt a modular architecture that facilitates scalability, maintainability and evolution of the product over time.

For a proprietary product, modularity is primarily a matter of speed and competitiveness. A well-structured architecture allows for the addition of features without increasing technical debt, scaling the solution to accommodate user growth, and facilitating the recruitment of new developers who can quickly understand and contribute to the code.

Modularity also facilitates customization for different customer segments or usage contexts, which is a direct commercial advantage for B2B or multi-sector solutions.

Associated best practices:

- Aim for a clear separation between the frontend, backend and database layers.
- Design independent, replaceable or extensible business modules without a complete overhaul.
- Externalize the configuration via environment variables rather than hardcoding it.

- **Anticipating increased load:** sizing the architecture to be able to scale horizontally if the user base grows.
- Design cross-functional components (authentication, notifications, billing) as reusable modules independent of the core business.

GUIDELINE 5 — Safety by Design

> **Recommendation:** It is recommended to integrate good security practices from the design and implementation of the solution, rather than treating them as a secondary step.

Security is a prerequisite for trust, whether the solution is intended for the public sector or the private market. A vulnerable solution exposes its users, damages the reputation of its developers, and can compromise the entire chain in which it is embedded. Integrating security from the outset is not only a best practice, but also a strong differentiating factor in the market.

Teams are encouraged to rely on recognized security frameworks (OWASP, best practices for secrets management, etc.) and to document the security choices made, in order to facilitate future audits.

Associated best practices:

- Implement authentication appropriate to the sensitivity level of the data processed (JWT, OAuth 2.0, etc.).
- Encrypt sensitive data in transit (HTTPS/TLS 1.2+) and consider encrypting it at rest.
- Never store sensitive data (passwords, API keys, credentials) in source code or Git repositories.
- **Rely on basic OWASP protections:** protection against SQL injection, XSS, CSRF, etc.
- Plan for logging sensitive actions with timestamps.
- Document a backup and restore procedure, even a simplified one.

GUIDELINE 6 — Transparency, Traceability & Data Protection

> **Recommendation:** It is recommended that the solution processes its users' data in a transparent, traceable and compliant manner with the principles of personal data protection.

User trust is a strategic asset for any private digital product . A solution that clearly explains how it uses data, allows its administrators to monitor system activity, and respects user rights will be more easily adopted, recommended, and retained.

Beyond trust, the protection of personal data is an increasingly essential requirement in African and international markets. Anticipating these requirements from the design stage avoids costly redesigns and favorably positions the solution with demanding clients or foreign partners.

Associated best practices:

- Set up an activity log for sensitive operations: creation, modification, deletion of data, connections.
- Collect only the data strictly necessary for the operation of the service (principle of data minimization).
- Clearly inform users about the data collected, its use, and their rights.
- Document the flows of personal data and the associated protection measures.
- Provide mechanisms allowing users to access, modify, or delete their data.

GUIDELINE 7 — Documentation & Skills Transfer

> **Recommendation:** It is recommended that the solution be accompanied by sufficient documentation to allow a local team to take ownership of it, maintain it and develop it further.

Documentation is often the neglected aspect of digital projects, yet it directly impacts the sustainability of a solution. A well-documented solution can be reused, improved, and passed on. It reassures organizations considering its adoption and facilitates the recruitment of new contributors or maintainers.

Within the context of the Djanta Tech Hub, which aims to strengthen Togo's digital ecosystem, the quality of documentation is also a sign of maturity and commitment to the local community. Teams are encouraged to document not only the technical operation of their solution, but also the architectural decisions that guided its development.

Associated best practices:

It is recommended to include the following documentary deliverables in the submission:

Document	Suggested content
README.md	Overview, prerequisites, quick start guide
Installation Guide	Step-by-step deployment or configuration
User guide	Manual for end users or customers
API documentation	OpenAPI (Swagger) specification of exposed endpoints
Contribution Guide	How to modify, configure or contribute to the solution

- Comment on the code or configuration files in complex parts, in French or English.
- Include validation tests to attest to the proper functioning of the solution (a coverage of at least 60% is encouraged for solutions developed).

GUIDELINE 8 — Creating Measurable Value

> **Recommendation:** It is recommended that each solution clearly articulate the value it creates, for its users or for the market, with concrete indicators.

A digital solution benefits from demonstrating its impact in a tangible way. Defining success indicators from the outset allows teams to better guide their development, prioritize high-impact features, and communicate convincingly with their future users, customers, or investors.

Djanta Tech Hub challenge values solutions that meet a real and documented need in the Togolese market or the sub-region, whether it is a sectoral issue, a daily use by citizens or businesses, or an identified market opportunity.

Associated best practices:

- **Present a concrete use case:** identified problem, target beneficiary, expected impact.
- **Define relevant success indicators:** number of users, time saved, error reduction, revenue generated, retention rate, etc.
- Anchor the solution in a documented need of the Togolese market or the sub-region.
- Consider integrating a dashboard or a monitoring mechanism, even a minimal one, to measure usage over time.