# RÈGLEMENT ET GUIDELINES TECHNIQUES

***Sommaire***

# RÈGLEMENT DU CONCOURS DES CHALLENGES DJANTA TECH HUB 2026

## PRÉAMBULE

Dans le cadre de la mise en œuvre de la Stratégie nationale Togo Digital et de la promotion de l'innovation technologique au Togo, le Djanta Tech Hub organise les challenges à l'attention de l'écosystème.

Ce concours national comprend deux programmes distincts et complémentaires :

- Djanta Innova – Challenge d'Innovation
- Djanta Idée-Action – Hackathon

Les challenges ont pour vocation d'identifier, de valoriser et d'accompagner des solutions innovantes répondant aux priorités nationales de développement dans des secteurs stratégiques.

## ARTICLE 1 : OBJECTIFS DU CONCOURS

Les challenges poursuivent les objectifs suivants :

1. Identifier des solutions innovantes à fort impact économique et social dans les secteurs prioritaires ;
2. Accompagner les équipes sélectionnées dans la structuration, le développement et la mise sur le marché de produits ou services viables ;
3. Contribuer au renforcement et à la structuration de l'écosystème national de l'innovation et de l'entrepreneuriat technologique.

## ARTICLE 2 : PROGRAMMES ET CONDITIONS D'ADMISSIBILITÉ

Les deux programmes portent notamment sur les secteurs suivants, sans que cette liste soit limitative : Agriculture, Éducation, Artisanat, Tourisme, Finance, Logistique, Productivité des PME, Optimisation des services publics et autres priorités nationales.

2.1 Djanta Innova (Challenge d'Innovation)

Le programme est ouvert aux startups, aux petites et moyennes entreprises (PME), aux entreprises sociales, aux entrepreneurs individuels, aux chercheurs, aux universitaires, aux professionnels ainsi qu'aux organisations non gouvernementales (ONG).

Les projets soumis doivent avoir atteint un niveau de maturité suffisant et disposer, au minimum, d'un prototype fonctionnel, d'un produit minimum viable (MVP) ou d'une solution techniquement démontrable.

2.2 Djanta Idée-Action (Hackathon)

Le programme s'adresse aux étudiants, aux jeunes diplômés ainsi qu'aux jeunes professionnels en début de carrière.

Les projets attendus doivent se situer au stade de l'idéation, qu'il s'agisse d'une phase de pré-idéation ou d'une idée initiale, sans qu'un prototype ou un produit minimum viable (MVP) ne soit requis à ce stade.

## ARTICLE 3 : CONDITIONS DE PARTICIPATION

### *3.1 Admissibilité générale*

Chaque candidat ou équipe ne peut soumettre qu'une seule candidature et à un seul programme.

Tous les membres des équipes doivent être citoyens togolais ou résidents légaux au Togo.

Les candidatures sont soumises en français ou en anglais. Les communications et présentations lors des bootcamps peuvent être faites également en français ou en anglais.

Les équipes sont composées de deux (2) à cinq (5) membres. Les candidatures individuelles sont admises pour le programme « Djanta Innova » même si la collaboration est fortement encouragée.

La participation d'équipes inclusives (genre, région, personnes vivant avec un handicap) est fortement encouragée.

### *3.2 Engagement des participants*

Tous les candidats s'engagent respecter le code de conduite du concours fondé sur la collaboration, le respect mutuel, l'éthique et l'originalité des projets.

Les participants sélectionnés s'engagent à prendre part à l'ensemble des activités du programme sélectionné (bootcamps, ateliers, séances de mentorat, événements finaux) ;

### *3.3 Originalité des projets et solutions*

Les projets soumis doivent être originaux et ne porter atteinte à aucun droit de propriété intellectuelle de tiers.

Les participants demeurent pleinement propriétaires de leurs idées, projets et solutions.

Les participants autorisent toutefois le Djanta Tech Hub à utiliser les informations relatives aux projets à des fins de communication, de promotion et de reporting institutionnel.

### *3.4 Motifs de disqualification*

Toute candidature pourra être disqualifiée en cas de :

- fourniture d'informations fausses ou trompeuses ;
- plagiat ou appropriation frauduleuse de concepts existants ;

- non-respect des délais, des règles du concours ou des engagements de participation.

## ARTICLE 4 : DOSSIER DE CANDIDATURE

### *4.1 Contenu des dossiers*

| Programme | Éléments requis |
|---|---|
| Djanta Innova | • Formulaire en ligne renseigné<br>• Description de la solution (300 mots maximum)<br>• Pitch deck<br>• Lien vers la démonstration ou design de l'interface utilisateur (pour MVP)<br>• Présentation de l'équipe<br>• CV ou profil LinkedIn du chef d'équipe (optionnel) |
| Djanta Idée-Action | • Formulaire de candidature avec informations sur l'équipe<br>• Résumé de l'idée initiale (500 mots maximum)<br>• Biographie des membres de l'équipe<br>• CV ou profil LinkedIn du chef d'équipe (optionnel) |

### *4.2 Modalités de soumission*

Les candidatures sont soumises exclusivement via la plateforme officielle à travers le lien fournit sur le site.

## ARTICLE 5 : CALENDRIER DU CONCOURS

Le calendrier du concours se déroule suivant ces étapes :

- Ouverture des candidatures : 27 Février 2026
- Clôture des candidatures : 10 Avril 2026
- Phase de présélection : 10 au 18 Avril 2026
- Bootcamps et sessions d'accompagnement : 27 et 28 Avril 2026
- Journée de pitch final : 30 Avril 2026
- Sélection finale : 01 Mai 2026

## ARTICLE 6 : PROCESSUS DE SÉLECTION PAR LE JURY

Les projets sont évalués par un jury indépendant sur la base des critères suivants :

1. Pertinence et alignement avec les priorités nationales ;

2. Caractère innovant et créatif de la solution ;
3. Potentiel d'impact économique et social ;
4. Qualité, complémentarité et engagement de l'équipe ;
5. Faisabilité technique et viabilité du projet.

**ARTICLE 7 : PRIX ET OPPORTUNITÉS**

***7.1 Djanta Innova – Projets lauréats***

Les équipes sélectionnées bénéficieront notamment de :

- l'accès au Bootcamp Challenge d'Innovation Djanta ;
- la participation à la Journée de pitch final ;
- l'intégration au programme d'incubation du Djanta Tech Hub ;
- un accompagnement comprenant mentorat, appui technique, accès au coworking et opportunités de financement ;
- une visibilité accrue auprès d'investisseurs et partenaires.

***7.2 Djanta Idée-Action – Meilleures équipes***

Les équipes retenues bénéficieront notamment de :

- la participation à un Sprint et Bootcamp Hackathon ;
- la Journée de pitch final ;
- l'accès à un programme de pré-incubation ;
- un accompagnement à la conception de MVP, mentorat, accès au coworking et opportunités de financement ;
- une visibilité institutionnelle et médiatique.

**ARTICLE 8 : PROPRIÉTÉ INTELLECTUELLE**

Les participants conservent l'intégralité des droits de propriété intellectuelle sur leurs projets.
Le Djanta Tech Hub est autorisé à utiliser leur travail à des fins de communication, de promotion et de reporting.

**ARTICLE 9 : PROTECTION DES DONNEES**

Conformément aux dispositions de la loi n° 2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel, les participants consentent uniquement, sur les bases juridiques concernées, à l'utilisation de leurs données à caractère personnel dans le cadre de communications ayant trait aux challenges du Djanta.

**ARTICLE 10 : RECLAMATIONS**

Les réclamations relatives à tout problème ou événement en lien avec les challenges ne sont recevables que dans une période de quinze (15) jours calendaires maximum à compter de la proclamation des résultats.

**ARTICLE 11 : ACCEPTATION DU RÈGLEMENT**

La soumission d'une candidature vaut acceptation pleine et entière du présent règlement. Tout participant s'engage à en respecter l'ensemble des dispositions.

TG

# GUIDELINES TECHNIQUES

Challenge Djanta Tech Hub

***Secteur du Challenge concerné : Service Public***

## Préambule

Ces guidelines s'adressent à toute équipe participant au challenge de développement d'applications et d'intégrations numériques organisé dans le cadre du lancement du Djanta Tech Hub. Elles constituent un cadre obligatoire visant à s'assurer que les solutions produites sont réutilisables, souveraines, interopérables et durables au sein de l'écosystème numérique national togolais.

Ces règles s'appliquent quelle que soit la nature de la contribution : développement d'une solution from scratch, configuration d'un outil existant, intégration de plusieurs briques logicielles, ou adaptation d'une solution open source. Elles ne doivent pas être appliquées de manière dogmatique, mais constituent un cadre formel de travail, un fil rouge que chaque équipe s'engage à respecter dans l'esprit comme dans la lettre.

## GUIDELINE 1 — Open Source & Standards Ouverts

> **Règle :** Toute solution soumise doit reposer sur des composants open source et être publiée sous une licence open source reconnue (MIT, Apache 2.0, GPL v3 ou EUPL).

L'usage de technologies open source est une condition non négociable pour toute solution destinée à l'administration publique togolaise. Cela garantit que l'État reste propriétaire de ses outils, peut les auditer librement, les faire évoluer et les confier à d'autres équipes sans être dépendant d'un fournisseur unique. Une solution sous licence propriétaire ne peut pas être considérée comme un bien public numérique.

Les formats de données, protocoles d'échange et interfaces exposées doivent également reposer sur des standards ouverts et documentés, accessibles à tout acteur de l'écosystème sans barrière technique ou commerciale.

**Ce que cela signifie concrètement :**

- Le code source ou les fichiers de configuration complets doivent être hébergés sur un dépôt public (GitHub, GitLab, Gitea, etc.) dès la soumission.
- Les formats de données utilisés (échanges, exports, stockage) doivent être des formats ouverts : JSON, XML, CSV, PDF/A, ODF — jamais des formats propriétaires verrouillés.
- Les protocoles d'API doivent respecter des standards ouverts : REST/JSON, GraphQL, OpenAPI 3.x.
- Aucune dépendance à un composant propriétaire non substituable n'est admise.

## GUIDELINE 2 — Déploiement On-Premise & Indépendance Infrastructurelle

> **Règle :** La solution doit pouvoir être déployée et opérée entièrement sur une infrastructure nationale, sans dépendance obligatoire à un service cloud tiers externe.

Les solutions numériques publiques ne peuvent pas reposer sur des infrastructures dont la continuité, la confidentialité et la localisation échappent au contrôle de l'État. Toute solution soumise doit donc être configurée et livrée de manière à fonctionner de façon autonome sur les infrastructures nationales disponibles, qu'il s'agisse de serveurs physiques, d'un data center gouvernemental ou d'un cloud souverain régional.

Si des services externes sont utilisés comme option, ils doivent être clairement identifiés et avoir une alternative locale documentée. La portabilité de la solution est un critère fondamental d'évaluation.

**Ce que cela signifie concrètement :**

- La solution doit être conteneurisée (Docker / Docker Compose obligatoire) pour permettre un déploiement reproductible sur n'importe quelle infrastructure.
- Elle ne doit pas requérir de connexion à des services cloud externes pour fonctionner (pas de dépendance obligatoire à AWS S3, Google Firebase, Azure AD, etc.).
- Si des services externes sont utilisés, ils doivent être substituables et documentés comme tels (ex. : stockage MinIO en remplacement local de S3).
- Un fichier docker-compose.yml permettant de lancer la totalité de la solution en une seule commande est obligatoire.
- La solution doit fonctionner dans un environnement faible bande passante si elle cible des usages terrain.

## GUIDELINE 3 — Interopérabilité & Intégration dans l'Écosystème National

> **Règle :** La solution doit être configurée et livrée de manière à s'intégrer dans l'écosystème numérique national (Xportal, Xflow, systèmes d'identification nationaux, etc.).

Une solution isolée, même techniquement excellente, n'a pas de valeur dans un écosystème public si elle ne peut pas communiquer avec les autres systèmes de l'État. L'interopérabilité n'est pas une fonctionnalité optionnelle — c'est une exigence structurelle. Chaque solution retenue dans le cadre du challenge doit être pensée comme un composant d'un écosystème plus large, capable d'échanger des données et de déléguer ou de consommer des services partagés.

Cette exigence s'applique aussi bien aux interfaces techniques (APIs) qu'aux modèles de données, qui doivent s'aligner sur les référentiels nationaux dès lors qu'ils existent.

**Ce que cela signifie concrètement :**

- Exposition ou activation d'une API REST documentée au format OpenAPI/Swagger.
- Support du protocole d'authentification OAuth 2.0 / OpenID Connect pour s'intégrer avec le système d'identité national.
- Toute entité métier échangée (citoyen, acte, demande, paiement) doit référencer un identifiant national normalisé si disponible.
- Un dictionnaire de données décrivant tous les champs exposés par l'API doit être fourni.
- Les notifications doivent pouvoir être routées vers les canaux nationaux (SMS, email, notification push) via des interfaces standardisées.

## GUIDELINE 4 — Architecture Modulaire & Réplicable

> **Règle :** La solution doit reposer sur une architecture modulaire permettant sa réutilisation, son adaptation et sa déclinaison à d'autres contextes administratifs ou à d'autres échelles.

L'investissement public dans le numérique n'a de sens que s'il peut être capitalisé et démultiplié. Une solution mise en place pour un ministère doit pouvoir être adaptée et déployée dans un autre contexte sans repartir de zéro. Cela implique une séparation claire des responsabilités au sein de l'architecture, une configuration externalisée, et une documentation permettant à une équipe tierce de comprendre, adapter et étendre la solution.

La modularité est également une garantie d'évolutivité : une architecture bien découpée permet d'intégrer de nouveaux modules ou de remplacer des composants sans déstabiliser l'ensemble du système.

**Ce que cela signifie concrètement :**

- Séparation claire frontend / backend / base de données avec des interfaces contractuelles définies.
- Les modules métier doivent être indépendants et remplaçables sans refonte globale.
- La configuration (environnement, URLs, clés) doit être externalisée via des variables d'environnement (fichier .env), jamais codée en dur.
- La solution doit inclure un guide d'adaptation expliquant comment la déployer pour un autre service ou une autre administration.
- Les composants génériques (authentification, notifications, audit log) doivent être exploitables comme des briques réutilisables.

## GUIDELINE 5 — Sécurité by Design

> **Règle :** La sécurité doit être intégrée dès le choix et la mise en place de la solution, et non traitée après coup.

Les systèmes publics numériques sont des cibles privilégiées. Une faille dans une solution peut compromettre des données de milliers de citoyens, nuire à la continuité du service public et éroder la confiance dans l'État. C'est pourquoi la sécurité ne peut pas être traitée comme un ajout tardif ou une couche superficielle : elle doit être une préoccupation centrale dès les premières décisions de configuration et d'architecture.

Chaque équipe est responsable d'intégrer les bonnes pratiques de sécurité à toutes les étapes de la mise en place de la solution, de la configuration de la base de données à la gestion des sessions utilisateurs, en passant par la protection des communications et la journalisation des actions sensibles.

**Ce que cela signifie concrètement :**

- Authentification forte obligatoire pour tout accès à des données personnelles ou sensibles (au minimum JWT signé, idéalement OAuth 2.0).
- Chiffrement des données sensibles en transit (HTTPS/TLS 1.2+) et au repos.
- Aucune donnée sensible (mots de passe, clés API, credentials) dans le code source ou les dépôts Git.
- **Activation des protections OWASP de base :** protection contre les injections SQL, XSS, CSRF, etc.

- Journalisation de toutes les actions sensibles avec horodatage — les logs doivent être consultables et non modifiables.
- Un plan de sauvegarde et de restauration simplifié doit être documenté.

## GUIDELINE 6 — Transparence, Traçabilité & Redevabilité

> **Règle :** Toutes les actions significatives dans le système doivent être traçables, auditables et compréhensibles par les parties prenantes concernées.

La confiance des citoyens dans les services publics numériques repose en grande partie sur leur capacité à comprendre ce qui est fait de leurs données et à vérifier que les processus sont équitables et honnêtes. Cela implique que toute décision automatisée soit explicable, que tout traitement de données personnelles soit justifié et documenté, et que les administrateurs disposent des outils nécessaires pour exercer une supervision effective du système.

La traçabilité n'est pas seulement une exigence réglementaire — c'est un mécanisme de gouvernance essentiel pour la gestion responsable d'un service public.

**Ce que cela signifie concrètement :**

- Activation d'un journal d'audit pour les opérations critiques : création, modification, suppression de données, connexions.
- Les algorithmes de décision automatique (si applicable) doivent être explicables et documentés.
- Les données personnelles collectées doivent être listées, justifiées et protégées conformément aux principes de minimisation des données.
- La solution doit permettre à un administrateur de consulter l'historique des actions sans possibilité d'altération des logs.
- Une documentation utilisateur claire doit expliquer comment les données sont utilisées.

## GUIDELINE 7 — Documentation & Transfert de Compétences

> **Règle :** La solution doit être suffisamment documentée pour qu'une équipe togolaise puisse la maintenir, la faire évoluer et la prendre en main de manière autonome, sans assistance extérieure.

La durabilité d'une solution numérique publique ne dépend pas uniquement de sa qualité technique initiale — elle dépend de la capacité des équipes nationales à en assurer la continuité dans le temps. Une solution non documentée est une solution fragile, dont la pérennité est conditionnée à la disponibilité de ses concepteurs ou intégrateurs originels. La documentation est donc un livrable à part entière, au même titre que le code ou les fichiers de configuration.

Cette exigence de transfert de compétences est également une manière concrète de contribuer au renforcement de l'écosystème numérique togolais sur le long terme.

### Ce que cela signifie concrètement :

La soumission doit impérativement inclure les documents suivants :

| Document | Contenu attendu |
|---|---|
| README.md | Présentation, prérequis, installation rapide |
| Guide d'installation | Déploiement ou configuration complet pas-à-pas |
| Guide utilisateur | Manuel pour les agents et/ou les citoyens |
| Documentation API | Spécification OpenAPI (Swagger) de tous les endpoints exposés |
| Guide de contribution | Comment modifier, configurer ou contribuer à la solution |

- Le code ou les fichiers de configuration doivent être commentés dans les parties complexes, en français ou en anglais.
- Des tests de validation doivent être inclus pour attester du bon fonctionnement de la solution (couverture minimale recommandée : 60 % pour les solutions développées).

## GUIDELINE 8 — Création de Valeur Publique Mesurable

> **Règle :** Chaque solution doit démontrer clairement la valeur qu'elle apporte aux citoyens ou à l'administration, avec des indicateurs mesurables.

Une initiative numérique dans le secteur public n'a de légitimité que si elle produit un impact réel et vérifiable sur la qualité du service rendu ou sur l'efficacité des processus administratifs. Il ne suffit pas qu'une solution soit techniquement correcte : elle doit répondre à un besoin

documenté, cibler une population bénéficiaire identifiée et définir dès le départ les indicateurs qui permettront d'évaluer son succès.

Cette orientation vers la valeur publique est ce qui distingue un projet d'innovation gouvernementale d'un simple exercice technique.

### Ce que cela signifie concrètement :

- **La soumission doit inclure un cas d'usage concret :** problème résolu, cible bénéficiaire, impact attendu.
- **Des indicateurs de performance (KPIs) doivent être définis :** nombre d'usagers, réduction du temps de traitement, taux d'erreur diminué, économies générées, etc.
- La solution doit répondre à un besoin documenté de l'administration ou des citoyens togolais.
- Un tableau de bord de suivi basique doit être intégré ou clairement prévu dans la roadmap.

# GUIDELINES TECHNIQUES

Challenge Djanta Tech Hub

***Secteurs du Challenge concernés : Agriculture, Education, Finance, Tourisme et culture, Commerce et artisanat, Logistique, Industrie créative, Productivité TPME***

# Préambule

Ces guidelines s'adressent aux équipes participant au challenge Djanta Tech Hub dont la solution est destinée au marché privé : startups, applications grand public, outils B2B, plateformes sectorielles, ou tout autre produit numérique qui répond à un besoin du marché togolais ou de la sous-région sans nécessairement interagir avec l'administration publique.

Elles constituent un cadre de référence, et non un cahier des charges rigide. Chaque équipe est encouragée à s'en inspirer selon la nature et la maturité de sa solution. Plus une solution s'alignera sur ces bonnes pratiques, plus elle sera robuste, maintenable, adoptable, et susceptible d'évoluer favorablement au sein de l'écosystème numérique régional.

## GUIDELINE 1 — Standards Ouverts & Interopérabilité Technique

> **Recommandation :** Il est recommandé que la solution s'appuie sur des standards techniques ouverts pour ses formats de données, ses protocoles d'échange et ses interfaces, afin de favoriser l'interopérabilité et d'éviter les dépendances techniques fermées.

Une solution privée n'a pas nécessairement vocation à publier son code source, et ce n'est pas ce qui est attendu ici. En revanche, le choix des formats et des protocoles techniques a un impact direct sur la capacité de la solution à s'intégrer avec d'autres outils, à être adoptée par des partenaires, et à évoluer dans le temps sans être prisonnière d'une technologie propriétaire.

S'appuyer sur des standards ouverts est un choix stratégique autant que technique : cela réduit les coûts d'intégration, élargit le bassin de développeurs capables de contribuer au projet, et facilite les partenariats commerciaux futurs.

**Bonnes pratiques associées :**

- Privilégier des formats de données ouverts pour les échanges et exports : JSON, XML, CSV, PDF/A.
- **Exposer des API basées sur des standards reconnus :** REST/JSON, GraphQL, OpenAPI 3.x.

- Éviter les formats ou protocoles propriétaires qui rendraient la solution difficilement intégrable par des tiers.
- Si une partie du code est générique et réutilisable, envisager de la publier en open source pour bénéficier des contributions de la communauté.

## GUIDELINE 2 — Portabilité & Évitement du Vendor Lock-in

> **Recommandation :** Il est recommandé de concevoir la solution de manière à ne pas créer de dépendances irréversibles à un seul fournisseur de services cloud ou d'infrastructure.

Le recours à des services cloud est tout à fait légitime pour une solution privée, et souvent même conseillé pour accélérer le développement et réduire les coûts opérationnels initiaux. Le risque à anticiper est celui du vendor lock-in : une dépendance trop forte à un fournisseur unique peut, à terme, contraindre les choix techniques, augmenter les coûts de manière imprévue, ou fragiliser la solution en cas de changement de conditions commerciales.

L'objectif n'est pas d'éviter le cloud, mais de conserver une marge de manœuvre stratégique. Une solution portable est une solution qui garde le contrôle de ses options.

**Bonnes pratiques associées :**

- Abstraire les dépendances aux services cloud (stockage, messagerie, authentification) derrière des interfaces substituables.
- Privilégier des services disposant d'alternatives open source ou multi-fournisseurs (ex. : S3-compatible, SMTP standard, OAuth standard).
- Envisager la conteneurisation (Docker / Docker Compose) pour faciliter la portabilité entre environnements.
- Documenter les dépendances externes et leurs alternatives potentielles.

## GUIDELINE 3 — Interopérabilité & Ouverture vers l'Écosystème

> **Recommandation :** Il est recommandé que la solution expose des interfaces permettant son intégration avec d'autres outils et services, afin de s'inscrire dans un écosystème numérique ouvert plutôt que de fonctionner en silo.

Une solution qui s'intègre facilement avec d'autres outils a un avantage compétitif réel : elle peut être adoptée plus rapidement, embarquée dans des workflows existants, et recommandée par

des partenaires. À l'inverse, une solution fermée crée des frictions à l'adoption et limite sa surface de marché.

L'interopérabilité est également un facteur de scalabilité : elle permet de déléguer certaines fonctions à des services spécialisés (paiement, identité, notification) plutôt que de tout reconstruire, ce qui accélère le développement et réduit la dette technique.

**Bonnes pratiques associées :**

- Exposer une API documentée au format OpenAPI/Swagger pour faciliter l'intégration par des partenaires ou des tiers.
- Prévoir des webhooks ou des mécanismes d'événements pour permettre à d'autres systèmes de réagir aux actions de la solution.
- S'appuyer sur des standards d'authentification reconnus (OAuth 2.0, OpenID Connect) pour faciliter les intégrations SSO.
- Fournir un dictionnaire de données ou une documentation des modèles exposés.
- Prévoir des connecteurs ou des guides d'intégration avec les outils les plus utilisés dans le secteur ciblé.

## GUIDELINE 4 — Architecture Modulaire & Scalable

> **Recommandation :** Il est recommandé d'adopter une architecture modulaire qui facilite la scalabilité, la maintenabilité et l'évolution du produit dans le temps.

Pour un produit privé, la modularité est avant tout un enjeu de vélocité et de compétitivité. Une architecture bien structurée permet d'ajouter des fonctionnalités sans dettes techniques croissantes, de faire monter en charge la solution face à une croissance des utilisateurs, et de recruter plus facilement de nouveaux développeurs qui pourront comprendre et contribuer rapidement au code.

La modularité facilite également la personnalisation pour différents segments de clients ou contextes d'usage, ce qui est un atout commercial direct pour les solutions B2B ou multi-secteurs.

**Bonnes pratiques associées :**

- Viser une séparation claire entre les couches frontend, backend et base de données.
- Concevoir des modules métier indépendants, remplaçables ou extensibles sans refonte globale.

- Externaliser la configuration via des variables d'environnement plutôt que de la coder en dur.
- **Anticiper la montée en charge :** dimensionner l'architecture pour pouvoir scaler horizontalement si la base d'utilisateurs croît.
- Concevoir les composants transverses (authentification, notifications, facturation) comme des modules réutilisables et indépendants du cœur métier.

## GUIDELINE 5 — Sécurité by Design

> **Recommandation :** Il est recommandé d'intégrer les bonnes pratiques de sécurité dès la conception et la mise en place de la solution, plutôt que de les traiter comme une étape secondaire.

La sécurité est un prérequis de confiance, que la solution soit destinée au secteur public ou au marché privé. Une solution vulnérable expose ses utilisateurs, nuit à la réputation de ses concepteurs et peut compromettre l'ensemble de la chaîne dans laquelle elle s'insère. Intégrer la sécurité dès le départ est non seulement une bonne pratique, c'est aussi un argument de différenciation fort sur le marché.

Les équipes sont encouragées à s'appuyer sur les référentiels de sécurité reconnus (OWASP, bonnes pratiques de gestion des secrets, etc.) et à documenter les choix de sécurité effectués, de manière à faciliter les audits futurs.

**Bonnes pratiques associées :**

- Mettre en place une authentification adaptée au niveau de sensibilité des données traitées (JWT, OAuth 2.0, etc.).
- Chiffrer les données sensibles en transit (HTTPS/TLS 1.2+) et envisager leur chiffrement au repos.
- Ne jamais stocker de données sensibles (mots de passe, clés API, credentials) dans le code source ou les dépôts Git.
- **S'appuyer sur les protections OWASP de base :** protection contre les injections SQL, XSS, CSRF, etc.
- Prévoir une journalisation des actions sensibles avec horodatage.
- Documenter une procédure de sauvegarde et de restauration, même simplifiée.

## GUIDELINE 6 — Transparence, Traçabilité & Protection des Données

**Recommandation :** Il est recommandé que la solution traite les données de ses utilisateurs de manière transparente, traçable et conforme aux principes de protection des données personnelles.

La confiance des utilisateurs est un actif stratégique pour tout produit numérique privé. Une solution qui explique clairement comment elle utilise les données, qui permet à ses administrateurs de suivre les activités du système et qui respecte les droits des utilisateurs sera plus facilement adoptée, recommandée et fidélisée.

Au-delà de la confiance, la protection des données personnelles est une exigence de plus en plus incontournable sur les marchés africains et internationaux. Anticiper ces exigences dès la conception évite des refontes coûteuses et positionne favorablement la solution face à des clients exigeants ou des partenaires étrangers.

**Bonnes pratiques associées :**

- Mettre en place un journal d'activité pour les opérations sensibles : création, modification, suppression de données, connexions.
- Collecter uniquement les données strictement nécessaires au fonctionnement du service (principe de minimisation).
- Informer clairement les utilisateurs sur les données collectées, leur usage et leurs droits.
- Documenter les flux de données personnelles et les mesures de protection associées.
- Prévoir des mécanismes permettant aux utilisateurs d'accéder à leurs données, de les modifier ou de les supprimer.

## GUIDELINE 7 — Documentation & Transfert de Compétences

**Recommandation :** Il est recommandé que la solution soit accompagnée d'une documentation suffisante pour permettre à une équipe locale de la prendre en main, la maintenir et la faire évoluer.

La documentation est souvent le parent pauvre des projets numériques, alors qu'elle conditionne directement la durabilité d'une solution. Une solution bien documentée peut être reprise, améliorée et transmise. Elle rassure les organisations qui envisagent de l'adopter et facilite le recrutement de nouveaux contributeurs ou mainteneurs.

Dans le contexte du Djanta Tech Hub, qui vise à renforcer l'écosystème numérique togolais, la qualité de la documentation est également un signal de maturité et d'engagement envers la

communauté locale. Les équipes sont encouragées à documenter non seulement le fonctionnement technique de leur solution, mais aussi les décisions d'architecture qui ont guidé sa construction.

### Bonnes pratiques associées :

Il est conseillé d'inclure dans la soumission les livrables documentaires suivants :

| Document | Contenu suggéré |
|---|---|
| README.md | Présentation, prérequis, guide de démarrage rapide |
| Guide d'installation | Déploiement ou configuration pas-à-pas |
| Guide utilisateur | Manuel à destination des utilisateurs finaux ou des clients |
| Documentation API | Spécification OpenAPI (Swagger) des endpoints exposés |
| Guide de contribution | Comment modifier, configurer ou contribuer à la solution |

- Commenter le code ou les fichiers de configuration dans les parties complexes, en français ou en anglais.
- Inclure des tests de validation pour attester du bon fonctionnement de la solution (une couverture d'au moins 60 % est encouragée pour les solutions développées).

## GUIDELINE 8 — Création de Valeur Mesurable

> **Recommandation :** Il est recommandé que chaque solution articule clairement la valeur qu'elle crée, pour ses utilisateurs ou pour le marché, avec des indicateurs concrets.

Une solution numérique gagne à démontrer son impact de façon tangible. Définir des indicateurs de succès dès le départ permet aux équipes de mieux orienter leur développement, de prioriser les fonctionnalités à fort impact, et de communiquer de manière convaincante auprès de leurs futurs utilisateurs, clients ou investisseurs.

Le challenge Djanta Tech Hub valorise les solutions qui répondent à un besoin réel et documenté du marché togolais ou de la sous-région, qu'il s'agisse d'une problématique sectorielle, d'un usage quotidien des citoyens ou des entreprises, ou d'une opportunité de marché identifiée.

**Bonnes pratiques associées :**

- **Présenter un cas d'usage concret :** problème identifié, cible bénéficiaire, impact attendu.
- **Définir des indicateurs de succès pertinents :** nombre d'utilisateurs, gain de temps, réduction d'erreurs, revenus générés, taux de rétention, etc.
- Ancrer la solution dans un besoin documenté du marché togolais ou de la sous-région.
- Envisager l'intégration d'un tableau de bord ou d'un mécanisme de suivi, même minimal, pour mesurer l'usage dans le temps.