


	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

REFERENTIEL DE GARANTIE « Numérique France Garanti »
Propriété de l'association Origine France Garantie

SOMMAIRE

- 1. PRESENTATION DE L'ASSOCIATION ORIGINE FRANCE GARANTIE**
 - 2. CONTEXTE ET OBJECTIF DE LA DEMARCHE DE GARANTIE NFG**
 - 3. LE CONTEXTE REGLEMENTAIRE**
 - 4. DOMAINE D'APPLICATION DE LA GARANTIE**
 - 5. LE REFERENTIEL DE GARANTIE**
 - 5.1 LES PRINCIPES GENERAUX DU SOCLE DU REFERENTIEL**
 - 5.2 LE PROCESSUS GENERAL DE DELIVRANCE ET DE SUIVI DE LA GARANTIE**
 - 6. MODIFICATION ET EXTENSION DU PERIMETRE DE GARANTIE**
 - 7. COMMUNICATION SUR L'OBTENTION DE LA GARANTIE**
 - 8. DECLINAISONS GEOGRAPHIQUES**
 - 9. ANNEXES SECTORIELLES**
- HISTORIQUE DES EVOLUTION DU REFERENTIEL DE GARANTIE**

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

1. PRESENTATION DE L'ASSOCIATION ORIGINE FRANCE GARANTIE

Créée en juin 2010, l'association Origine France Garantie a l'ambition de réunir les entreprises et plus largement tous les acteurs qui souhaitent participer à l'élaboration d'un schéma de garantie volontaire, innovant et transparent de l'origine française des produits, des services et des solutions numériques.

La création de trois schémas de garantie (Origine France Garantie, Service France Garanti et Numérique France Garanti), certifiées par des organismes indépendants et reconnus, répond aux attentes exprimées par les consommateurs, par les entreprises et de nombreuses fédérations professionnelles.

L'association Origine France Garantie a pour objet la défense et la valorisation des produits de fabrication française, qu'il s'agisse de biens ou de services et des entreprises qui les produisent ainsi que la promotion de l'« Origine France Garantie » dans tous les secteurs d'activité, sur le marché intérieur comme à l'export.

L'association dispose de plusieurs moyens de communication pour faire connaître Origine France Garantie :

- Le trimestriel Produire en France magazine imprimé à hauteur de 10 000 exemplaires et distribué dans les kiosques partout en France.
- Participation à de nombreux évènements : MIF Expo, tables rondes, conférences, salons professionnels, etc.
- Communication digitale (réseaux sociaux et site internet).
- Campagnes de publicité.

Coordonnées complètes d'Origine France Garantie



Association Origine France Garantie
38 bis, rue Fabert
75007 Paris
T : 01 40 62 70 56
www.originefrancegarantie.fr
contact@originefrancegarantie.fr

Déclaration

Identification R.N.A. : W751205121
No de parution : 20100025
Département (Région) : Paris (Île-de-France)
No d'annonce : 1878
Paru le : 19/06/2010

Références Insee

Inscription au répertoire SIRENE : 05/2010

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

Identifiant SIREN : 523 645 299

Identifiant SIRET du siège : 523 645 299 00042

Catégorie juridique : Association déclarée

Activité Principale Exercée (APE) : 9499Z - Autres organisations fonctionnant par adhésion volontaire

2. CONTEXTE ET OBJECTIF DE LA DEMARCHE DE GARANTIE NFG

2.1 Contexte

Le numérique est devenu un enjeu stratégique majeur, au cœur du fonctionnement de l'économie, des services publics et de la vie démocratique. Les infrastructures numériques, les logiciels, les données et les algorithmes constituent désormais des actifs critiques, au même titre que les infrastructures industrielles traditionnelles.

Dans ce contexte, la France et plus largement l'Europe font face à une dépendance croissante vis-à-vis d'acteurs extra-européens. Une part significative des dépenses numériques est aujourd'hui captée par des entreprises étrangères, entraînant une fuite de valeur, d'innovation, d'emplois et de recettes fiscales hors du territoire. Cette situation fragilise la capacité des acteurs économiques et publics à maîtriser leurs technologies, leurs données et, plus largement, leur autonomie stratégique.

Parallèlement, le développement rapide des offres numériques s'accompagne d'un manque de lisibilité sur l'origine réelle des solutions proposées. De nombreuses communications commerciales mettent en avant des notions telles que « souveraineté », « cloud de confiance » ou « solution européenne », sans qu'il n'existe de cadre harmonisé permettant d'en vérifier la réalité. Cette situation favorise des pratiques assimilables à du « francolavage », susceptibles d'induire en erreur les utilisateurs, qu'ils soient publics ou privés.



Dans ce contexte, et à l'instar des constats ayant conduit à la création des Marques de Garantie Origine France Garantie pour les produits et Service France Garantie pour les services, il apparaît nécessaire de définir un cadre clair, exigeant et vérifiable permettant de caractériser l'origine française d'une solution numérique.

Numérique France Garantie s'inscrit dans cette dynamique. Il vise à apporter une réponse structurée aux enjeux de transparence, de compétitivité et de souveraineté, en proposant un référentiel fondé sur des critères objectifs, audités par un organisme indépendant.

2.2 Objectifs

Le référentiel de garantie Numérique France Garantie poursuit plusieurs objectifs :

- ▶ **Renforcer la souveraineté numérique française** en favorisant la maîtrise nationale des technologies critiques, de leur conception à leur exploitation, ainsi que de la valeur économique associée.
- ▶ **Valoriser les acteurs du numérique ancrés en France** en leur proposant une démarche professionnelle, structurée et crédible, leur permettant de démontrer leur contribution à l'économie nationale, sur le marché intérieur comme à l'export.
- ▶ **Délivrer aux utilisateurs une information fiable, sincère et transparente** sur l'origine des solutions numériques qu'ils utilisent, en dépassant les déclarations marketing au profit de critères objectivés et vérifiés.

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

► **Structurer un écosystème numérique responsable et durable** en encourageant la relocalisation des activités, le développement des compétences et la création d'une chaîne de valeur sur le territoire.

► **Mettre en place un cadre de référence transversal, homogène et évolutif** applicable à l'ensemble des acteurs de la chaîne de valeur du numérique, et compatible avec les évolutions réglementaires nationales et européennes.

Il est important de noter que cette démarche d'évaluation de la conformité au référentiel est une démarche volontaire, à l'initiative des entreprises.

2.3 Principes de la démarche

Cette démarche se veut efficace et repose sur les principes suivants :

1. **Une démarche porteuse de valeurs et facilement identifiable**

Elle garantit que la valeur ajoutée numérique est réalisée en France et que les activités essentielles (conception, développement, gouvernance, hébergement des données) sont localisées et maîtrisées sur le territoire national.

2. **Une démarche compréhensible et pragmatique**

Sa mise en œuvre est adaptée aux spécificités des activités numériques et accessible aux entreprises, quelle que soit leur taille ou leur domaine (éditeurs de logiciels, plateformes, cloud, intelligence artificielle, cybersécurité, services numériques, etc.).

3. **Une démarche structurante pour la filière numérique**

Elle permet d'articuler les différentes composantes de la chaîne de valeur (infrastructures, logiciels, gestion des données, usages) dans une approche cohérente et industrielle.

4. **Un système de suivi reconnu garantissant la crédibilité de la démarche**



- En France et à l'international,
- Reposant sur des audits indépendants mené par un Organisme Certificateur,
- S'appuyant sur des outils de traçabilité et de transparence accessibles aux utilisateurs

3. CONTEXTE REGLEMENTAIRE

3.1. Contexte réglementaire Numérique France Garanti

L'obtention de l'attestation de conformité au référentiel et l'utilisation de la marque associée supposent le respect par l'entreprise de l'ensemble des lois et réglementations auxquelles elle est soumise, en particulier le code du travail, le code douanier, les réglementations relatives à l'hygiène, à la sécurité, à l'environnement, etc. Cependant, les audits n'ont pour objet que de vérifier le respect par l'entreprise du référentiel pour ce qui concerne les solutions numériques soumis à évaluation.

En cas de non-respect flagrant par l'entreprise de l'une de ses obligations essentielles, le Comité Technique de la Marque pourra décider de suspendre tout ou partie des certificats décernés à l'entreprise concernée s'il estime que la défaillance de l'entreprise est susceptible

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

de porter atteinte à la réputation de l'Association Origine France Garantie ou à ses trois schémas de garantie (Origine France Garantie, Service France Garanti et Numérique France Garanti).

L'approche méta-standard adoptée pour construire le référentiel permet la reconnaissance et le respect des autres schémas existants.

3.2. Définitions

Au sens du présent référentiel, les termes suivants sont définis comme suit :

Solution numérique : Ensemble cohérent de composants logiciels, de services, de données et d'infrastructures permettant de fournir une fonctionnalité ou un service numérique identifié.

Gamme de solutions : Ensemble de solutions numériques reposant sur une base technique, fonctionnelle ou organisationnelle commune.

Périmètre de l'attestation de conformité au référentiel : Ensemble constitué par une organisation et une ou plusieurs solutions numériques faisant l'objet de la garantie.

Activités clés : Ensemble des activités nécessaires à la conception, au développement, à l'exploitation, à la sécurisation et à la maintenance d'une solution numérique.

Souveraineté numérique : Capacité d'une organisation à maîtriser ses solutions numériques, ses données, ses infrastructures et les technologies associées, dans un cadre garantissant leur indépendance vis-à-vis de toute législation extraterritoriale susceptible d'en affecter l'intégrité, la confidentialité ou la disponibilité.

Dépendance critique : Dépendance à un composant, un service ou une technologie dont la maîtrise est indispensable au fonctionnement de la solution et dont l'absence de contrôle peut compromettre la souveraineté, la sécurité ou la continuité d'activité.

Valeur ajoutée numérique : Ensemble des coûts et contributions mobilisés pour la conception, le développement, l'exploitation et la maintenance d'une solution numérique.



→ Précision pour le périmètre 2 ?

Chaîne d'approvisionnement numérique : Ensemble des fournisseurs, prestataires/sous-traitants, outils, logiciels, infrastructures et services contribuant à la réalisation et à l'exploitation d'une solution numérique.

Adhérence : Niveau de dépendance de la solution numérique à un prestataire, fournisseur, outil technologique ou composant.

Elle est évaluée au regard :

- du coût de remplacement,
- du délai nécessaire à la substitution,

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

- de la complexité technique induite,
- et de l'impact opérationnel sur la continuité d'activité.

Une adhérence faible traduit l'existence d'alternatives facilement mobilisables ; dans ce cas, les coûts associés sont pleinement pris en compte dans l'évaluation du critère relatif à la localisation de la valeur ajoutée.

À l'inverse, une adhérence forte caractérise une dépendance critique, susceptible d'affecter la souveraineté, la sécurité, la résilience ou la maîtrise technologique de la solution. Ces dépendances font l'objet d'une analyse spécifique dans le cadre du critère de souveraineté. La notion d'adhérence permet ainsi d'ajuster l'évaluation des dépendances et des coûts en fonction du caractère substituable ou structurant des éléments considérés.

Les modalités précises d'appréciation de l'adhérence sont définies et affinées dans le cadre des audits, notamment **lors de la phase pilote du référentiel**.

Elle peut être appréciée qualitativement ou, lorsque pertinent, faire l'objet d'une évaluation structurée selon une grille définie par le certificateur.

4. DOMAINES D'APPLICATION DU RÉFÉRENTIEL

Numérique France Garanti s'applique à des **solutions numériques ou à des gammes de solutions numériques**, développées, opérées ou fournies par une organisation.

Elle ne s'applique pas à l'ensemble de l'entreprise, mais porte sur un **périmètre clairement défini de solutions**, pour lesquelles l'organisation candidate est en mesure de démontrer le respect des exigences du présent référentiel.

Chaque attestation de conformité est ainsi attribuée à :



- une **solution numérique identifiée**,
- ou une **gamme cohérente de solutions numériques**, associée à une organisation responsable de sa conception, de son développement, de son exploitation ou de sa fourniture,
- ou à une infrastructure physique d'hébergement de données.

4.1 Définition du périmètre

Le périmètre couvert par l'attestation de conformité doit être défini de manière précise par l'organisation candidate. Il comprend :

- la ou les **solutions numériques concernées**,
- les **activités associées** (conception, développement, exploitation, maintenance),
- les **ressources mobilisées** (humaines, techniques),
- les **infrastructures utilisées**,
- ainsi que les éventuels **prestataires et fournisseurs**

L'organisation doit démontrer la maîtrise de ce périmètre ainsi que la traçabilité des activités associées.

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

4.2 Typologie des solutions numériques couvertes

Afin de couvrir l'ensemble de la chaîne de valeur du numérique tout en garantissant une lecture claire et non ambiguë, le référentiel est structuré selon les périmètres suivants :

Périmètre 1 – Solutions logicielles, applications et services cloud

Ce périmètre couvre les solutions numériques reposant sur des développements logiciels ou des services numériques, incluant notamment :

- logiciels (SaaS, on-premise, hybrides),
- applications web et mobiles,
- plateformes numériques,
- services cloud applicatifs.

Il inclut l'ensemble des activités de conception, développement, intégration, exploitation et maintenance associées à ces solutions.

Périmètre 2 – Infrastructures d'hébergement (data centers)

Ce périmètre couvre exclusivement les **infrastructures physiques d'hébergement des données**, incluant :

- data centers,
- moyens techniques d'exploitation associés (serveurs, réseaux internes, équipements critiques).

L'évaluation porte sur la localisation, la maîtrise des flux et l'exploitation des infrastructures physiques supportant les services numériques, ainsi que la structure des coûts associés.

Périmètre 3 – Solutions de conseil et de transformation numérique

Ce périmètre couvre les solutions intégrant une composante de conseil ou d'accompagnement à la transformation digitale, dès lors qu'elles reposent sur des **livrables numériques identifiables**, tels que :

- plateformes,
- outils digitaux,
- systèmes d'information.

Périmètre 4 – Solutions de cybersécurité et infrastructures réseaux

Ce périmètre couvre les solutions contribuant à la sécurité et au bon fonctionnement des systèmes numériques, incluant :

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

- outils et services de cybersécurité,
- solutions de protection des données,
- infrastructures et services réseaux.

4.3 Principe de non-chevauchement des périmètres

Chaque solution doit être rattachée à un périmètre principal en fonction de son activité dominante.

Lorsque plusieurs périmètres sont concernés, l'organisation doit identifier le périmètre principal, expliciter les interactions avec les autres périmètres, et démontrer la cohérence globale du périmètre certifié.

4.4 Exclusions et limites

Ne peuvent faire l'objet d'une attestation de conformité :

- les organisations en tant que telles, sans périmètre de solution défini,
- les solutions dont le périmètre n'est pas clairement identifiable,
- les activités ne relevant pas du champ numérique.

5. LE REFERENTIEL

Le référentiel Numérique France Garanti est constitué d'un socle et d'annexes sectorielles qui déclinent des critères spécifiques pour chaque secteur lié au numérique.

5.1 LES PRINCIPES GÉNÉRAUX DU SOCLE DU RÉFÉRENTIEL



Numérique France Garanti repose sur un ensemble de principes visant à garantir, de manière objective et vérifiable, l'origine française des solutions numériques au regard de critères de souveraineté, de sécurité et de production de valeur.

Il s'inscrit dans une logique de structuration de l'écosystème numérique français, en apportant un cadre de référence commun, lisible et crédible pour les entreprises, les acteurs publics et les utilisateurs.

Dans la continuité des démarches de garantie portées par l'association, Numérique France Garanti est construit en adaptant les principes de l'association aux spécificités des activités numériques, notamment en matière de dépendances technologiques, de circulation des données et de structuration de la chaîne de valeur.

Numérique France Garanti s'applique à une organisation pour une solution numérique ou une gamme de solutions clairement identifiée.

Dans le cadre de sa version initiale, le référentiel s'appuie sur une phase pilote permettant de tester, d'ajuster et de consolider les exigences définies. Les retours des entreprises

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

auditées dans ce cadre ont vocation à enrichir et faire évoluer le référentiel vers une version stabilisée.

Le référentiel repose sur deux critères cumulatifs, comme suit :

- **Critère A – Souveraineté numérique, localisation des activités clés et protection des données**
- **Critère B – Une valeur ajoutée acquise majoritairement en France.**

Le respect simultané de ces deux critères conditionne l’obtention et le maintien de l’attestation.

5.1.1 Critère A – Souveraineté numérique, localisation des activités clés et protection des données



Ce critère vise à garantir que la solution numérique certifiée est conçue, développée et exploitée dans des conditions assurant la maîtrise effective de ses technologies, de ses données et de ses infrastructures.

À ce titre, l’organisation doit démontrer :

- une **souveraineté technologique**, impliquant l’absence de dépendance critique non maîtrisée vis-à-vis de technologies ou de législations extraterritoriales,
- une **gouvernance et une juridiction française**, garantissant que les décisions stratégiques, techniques et opérationnelles sont prises en France,
- une **localisation des activités clés sur le territoire français**,
- une **infrastructure d’hébergement conforme aux exigences de localisation**, incluant, pour les infrastructures physiques, la maîtrise des sites, des opérations et des accès.
- une **traçabilité de l’origine des données**, dans un cadre conforme aux exigences réglementaires applicables,
- une **gouvernance des systèmes d’intelligence artificielle**, lorsque applicable, garantissant la maîtrise des modèles et de leurs dépendances, leur origine et leur intégration dans un environnement sous contrôle français, ainsi que la mise en place de dispositifs assurant la transparence, la traçabilité et la maîtrises des risques dans le temps,
- la mise en œuvre de **mesures organisationnelles et techniques** relatives :
 - à la protection des données,
 - à la sécurité des systèmes d’information,
 - à la continuité d’activité et à la résilience.

Le critère A intègre également l’**analyse des activités externalisées**, en tenant compte du niveau d’adhérence des prestataires et fournisseurs. Cette analyse doit démontrer qu’**au moins 80% de ces dépenses** sont réalisés par des **partenaires sous contrat français et basés en France**.

Il implique enfin une **orientation majoritaire des investissements** sur le territoire français.

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

Il vise à garantir que la solution numérique certifiée est maîtrisée sur le territoire français, tant sur le plan technique que juridique, et qu'elle est exploitée dans des conditions assurant la protection des données et l'indépendance technologique.

5.1.2 Critère B – Une valeur ajoutée acquise majoritairement en France

Le critère B vise à garantir que la solution numérique certifiée contribue de manière significative à la création de valeur et d'emplois en France.

Il repose sur l'évaluation de la localisation de l'acquisition de la valeur ajoutée, en prenant en compte l'ensemble des postes de dépenses nécessaires à la réalisation et à l'exploitation de la solution numérique.

Sont notamment considérés :

- La contribution des équipes techniques (développeurs, opérateurs de plateforme, ergonomes, experts en sécurité applicative, chefs de projets IT, techniciens support,...),
- Les dépenses de formation associées,
- Les masses salariales chargées de l'encadrement et des fonctions support,
- Les prestations techniques externalisées,
- La chaîne d'approvisionnement en outils et moyens opérationnels,
- Les dépenses de recherche et développement,
- Le budget consacré à la propriété intellectuelle,
- Ainsi que les coûts d'infrastructure, incluant les investissements matériels, l'exploitation, la maintenance et l'énergie.

Ces éléments sont analysés en tenant compte, lorsque pertinent, du niveau d'adhérence des prestataires et fournisseurs.

Le référentiel exige que la majorité de cette valeur soit réalisée en France. Dans le cadre de la version initiale du référentiel, ce seuil est fixé à :

- **60 % minimum** pour les périmètres 1, 3 et 4,
- **50 % minimum** pour le périmètre 2.



Ces seuils sont susceptibles d'évoluer à l'issue de la phase pilote.

5.1.3 Principes de mise en œuvre

La mise en œuvre des critères repose sur les principes suivants :

- **Principe de traçabilité et de justification**

L'organisation doit être en mesure de justifier l'ensemble des éléments pris en compte, à l'aide de preuves documentées. Cela implique la capacité de justifier l'origine des activités, des données, des composants et des dépenses considérés dans l'évaluation.

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

- **Principe de transparence**

Les informations communiquées doivent être sincères, cohérentes et vérifiables.

- **Principe d’auditabilité**

L’ensemble des éléments déclarés doit pouvoir faire l’objet de vérifications dans le cadre d’un audit indépendant, comprenant une vérification documentaire et, le cas échéant, un audit sur site ou environnement technique selon l’analyse de risques.

- **Principe de maintien de la conformité**

Le respect des exigences du référentiel doit être assuré dans la durée, pendant toute la période de validité de l’attestation. Des audits de suivi réguliers garantissent le maintien de cette conformité.

- **Principe de prise en compte des dépendances**

Les relations avec les prestataires et fournisseurs sont analysées au regard de leur niveau d’adhérence.

- **Principe d’inclusivité et de progressivité**

Le schéma de garantie vise à structurer l’écosystème numérique français en permettant l’entrée d’acteurs de tailles et de maturités variées, dans une logique d’amélioration continue.

Cas spécifique du périmètre 2 – Infrastructures d’hébergement

Pour les solutions relevant du périmètre 2, les critères A et B sont interprétés en tenant compte des spécificités des infrastructures physiques d’hébergement.

À ce titre :

- Les activités clés s’entendent principalement comme les activités d’exploitation, de maintenance, de sécurisation et de supervision des infrastructures,
- La souveraineté s’apprécie notamment au regard de la localisation physique des infrastructures, du contrôle des opérations, et de la gouvernance des données hébergées,
- La valeur ajoutée prend en compte les coûts liés aux infrastructures (investissements, exploitation, maintenance, énergie, loyers des bâtiments, personnel technique).



Les modalités d’évaluation détaillées sont précisées, le cas échéant, dans les annexes sectorielles.

5.2 PROCESSUS GÉNÉRAL DE DÉLIVRANCE ET DE SUIVI DE LA GARANTIE

5.2.1 Dossier de candidature

NB : l’ensemble des informations communiquées à l’Organisme Certificateur sont traitées en totale confidentialité.

Ce dossier est constitué par le demandeur et adressé à un Organisme Certificateur agréé par l’association Origine France Garantie.

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

Le demandeur est l'entreprise qui souhaite faire reconnaître sa solution numérique NFG et qui s'engage à la fournir à un client.

Le demandeur est l'interlocuteur de l'Organisme Certificateur et, à ce titre, a la responsabilité de la constitution et la communication du dossier complet de candidature.

L'organisation candidate dépose un dossier de candidature en définissant le périmètre de la solution ou de la gamme de solutions concernée. Une phase d'autoévaluation peut être réalisée en amont, afin de vérifier l'éligibilité de la solution.

Le dossier fait l'objet d'une analyse visant à vérifier sa complétude, la cohérence du périmètre déclaré et la recevabilité de la demande. Dans ce cadre, des échanges peuvent intervenir afin de préciser ou compléter les éléments fournis.

CONSTITUTION DU DOSSIER DE CANDIDATURE



5.2.1.1 Informations générales

- Identification de la société : nom, adresse, N° Siret, secteur d'activité concerné par la demande.
- Identification de l'interlocuteur du certificateur : Nom, Prénom, fonction, n° de téléphone, courriel.
- Identification de la solution ou des gammes de solutions numérique(s) concernée(s) par la candidature, accompagnée des fiches commerciales et/ou technique.
- Le demandeur précise le volume et le chiffre d'affaires annuel générés par la solution numérique, ainsi que le nombre de salariés concourant à sa réalisation.

5.2.1.2 Informations générales sur le processus de production de la solution numérique

- Pour chaque gamme de solution numérique, le demandeur communique un schéma précisant **l'ensemble** des étapes du processus de production menant à la solution (que ces étapes soient sous sa responsabilité ou non).
- Le demandeur devra également préciser les métiers des personnes intervenant dans la mise en œuvre de la solution numérique ainsi que le nombre de salariés intervenants.
- Pour chacune des étapes du processus de production, le demandeur communique une évaluation exprimée en pourcentage, de l'impact de cette étape sur la valeur de la solution numérique objet de l'attestation.
- Le demandeur précise le cas échéant les informations gérées par outils de gestion de projet et susceptibles de justifier les points précédents.

5.2.1.3 Informations spécifiques sur le processus de production de la solution

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

- Le demandeur identifie les étapes du processus de production placées sous sa responsabilité incluant la dernière ouvraison ; il précise ce qu'il considère être l'étape où le produit prend ses caractéristiques essentielles (on entend par « placées sous sa responsabilité » les opérations effectuées sur ses sites ou environnements techniques propres ainsi qu'en sous-traitance contractuelle).
- Pour chacune des étapes précédentes, le demandeur précise les lieux d'intervention (adresse du site ou localisation de l'environnement technique, contact possible...), mais également le nom, l'adresse et le contact de ses prestataires ou sous-traitants chargés des différentes opérations menant à la réalisation de la solution numérique et de toute autre partie du processus de mise en œuvre pris en compte pour la démarche.

Il confirme l'existence d'un lien avec ses prestataires incluant :

- Un bon de commande précisant les actions réalisées,
- Une fiche technique,
- Idéalement un contrat de prestation ou de sous-traitance.

Ces documents doivent être à la disposition de l'Organisme Certificateur lors des audits. Le demandeur précise à l'Organisme Certificateur la ou les périodes de développement ou exploitation pour ses sites mais également les plannings convenus avec ses prestataires ou sous-traitants.

Informations particulières relatives aux prestataires ou sous-traitants, à obtenir par le Demandeur et à communiquer :

Le prestataire ou sous-traitant dispose-t-il d'un ou plusieurs site(s) physique(s) de développement ou exploitation ? Si oui, préciser sa/leurs localisation(s).

Le prestataire ou sous-traitant est-il autorisé par le Demandeur à sous-traiter une ou plusieurs opérations ? Si oui, préciser les sites de développement ou exploitation et lieux possibles de sous-traitance. En cas de recours à un sous-traitant non prévu, l'Organisme Certificateur doit être informé sans délai. Le cas échéant, la procédure d'attestation pourra si nécessaire être adaptée.

Le demandeur, en prenant appui sur les précisions précédentes, justifie le respect des critères A et B le rendant légitime à la demande de candidature.

5.2.1.4 Informations sur la traçabilité et l'autocontrôle

Le demandeur décrit les dispositifs mis en œuvre afin d'assurer la traçabilité, le contrôle et la maîtrise des éléments constitutifs de la solution numérique certifiée.

Traçabilité de la solution numérique

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

- Le demandeur précise le système de traçabilité mis en place permettant d'identifier et de suivre :
 - Les composants logiciels (code source, bibliothèques, dépendances, ...),
 - Les infrastructures et environnements d'exécution,
 - Les données utilisées (collecte, traitement, stockage),
 - Les prestataires et fournisseurs intervenant dans la chaîne de valeur.
- Il fournit un inventaire structuré des composants et dépendances de la solution (incluant, le cas échéant, un SBOM ou équivalent), permettant d'identifier leur provenance et leur localisation.
- Le demandeur décrit les flux de données associés à la solution (collecte, stockage, traitement, sauvegarde), ainsi que leur localisation.

Systemes de contrôle et de maîtrise

- Le demandeur décrit les dispositifs de contrôle permettant de garantir :
 - La conformité de la solution aux exigences du présent référentiel,
 - La maîtrise des évolutions techniques (mises à jour, changements d'architecture, intégration de nouveaux composants, ...)
 - La cohérence entre les caractéristiques annoncées et les conditions réelles d'exploitation.
- Il précise les mesures mises en œuvre en matière :
 - De sécurité des systèmes d'information,
 - De protection des données,
 - De continuité d'activité.



Autocontrôle et gestion des risques

- Le demandeur décrit les mécanismes d'autocontrôle et de surveillance interne permettant d'identifier :
 - Les éventuelles non-conformités,
 - Les évolutions susceptibles d'affecter la souveraineté, la sécurité ou la localisation de la solution,
 - Les dépendances critiques.
- Il précise les procédures mises en place pour :
 - Détecter, analyser et corriger les incidents,
 - Maintenir la conformité dans le temps,
 - Assurer la traçabilité des actions correctives.

Cas des systèmes intégrant de l'intelligence artificielle

Lorsque la solution intègre des composants d'intelligence artificielle, le demandeur précise les dispositifs permettant d'assurer :

- La traçabilité des données utilisées pour l'entraînement et l'exploitation des modèles,
- La maîtrise des modèles et de leurs dépendances,
- L'identification et le suivi des risques liés aux biais ou aux dérives, et
- Les mécanismes de supervision et de mise à jour des modèles.

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

5.2.1.5 Informations générales sur les reconnaissances qualité et cybersécurité existantes

- Le demandeur précise, et donne copie, des certifications ou labels dont il bénéficie ainsi que ses sous-traitants (ex : certifications ISO, SecNumCloud, de cybersécurité ou sectorielles, ...) en lien avec les solutions ou les sites ou environnements techniques concernés par la demande de candidature.
- Une liste des labels et des référentiels concernés sera annexée au présent document dans la partie « référentiel sectoriel ».

5.2.1.6 Cas particulier des filières et syndicats professionnels

Afin de simplifier la constitution du dossier de demande, il est convenu que les entreprises organisées en filières, groupements, syndicat professionnel, etc. pourront faire valider un schéma type de l'ensemble du processus de mise en œuvre d'une solution numérique ou d'une gamme de solutions numériques. Ce schéma global concerté identifiera les étapes nécessairement maîtrisées par tout candidat dans ce secteur d'activité.

Les étapes ainsi imposées par la profession répondront aux critères A et B du référentiel. En conséquence, le demandeur s'attachera à justifier la maîtrise de ces étapes.

5.2.1.7 Modification et extension du périmètre de garantie :

5.2.1.7.1 Modification de la demande :



Pour une demande ayant fait l'objet de la remise d'un dossier et d'une procédure en cours par le certificateur, on entend par modification toute évolution susceptible d'affecter les conditions d'évaluation de la solution numérique.

Sont notamment considérées comme des modifications :

- Un changement d'architecture technique ou des composants principaux de la solution,
- Un changement d'infrastructure d'hébergement ou de la localisation des données,
- L'introduction ou la modification de dépendances technologiques critiques,
- Un changement significatif dans les prestataires ou sous-traitants intervenant dans la solution,
- Une évolution des systèmes d'intelligence artificielle utilisés, le cas échéant,
- Une modification de la gouvernance ou des conditions d'exploitation de la solution.

Ces nouveaux éléments sont à porter, sans délai, à la connaissance du certificateur qui pourra adapter la procédure d'évaluation.

5.2.1.7.2 Extension de la démarche sans modification du périmètre :

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

Le demandeur peut étendre sa démarche à une nouvelle solution ou fonctionnalité, dans le cadre d'un périmètre existant, dès lors que :

- La nouvelle solution repose sur une architecture technique identique ou équivalente,
- Les activités clés sont réalisées dans des conditions similaires,
- Les infrastructures d'hébergement et de traitement des données sont inchangées,
- Les prestataires, fournisseurs et dépendances critiques restent identiques ou équivalents.

Dans ce cas, le dossier de demande peut être simplifié et présenté sous forme d'un complément au dossier initial.

Ce complément précise notamment :

- L'identification de la solution ou fonctionnalité ajoutée
- Son rattachement au périmètre existant
- Les éléments justifiant l'absence de modification de la conformité aux critères A et B.

5.2.1.7.3 Extension de la démarche avec modification du périmètre :

Une nouvelle demande complète est requise lorsque l'extension concerne une solution ou un périmètre présentant des différences significatives, notamment :

- Une architecture technique distincte,
- Des activités clés différentes ou localisées différemment,
- Un recours à de nouveaux prestataires ou fournisseurs structurants,
- Une modification des conditions d'hébergement ou de traitement des données,
- Une évolution substantielle des dépendances technologiques ou des systèmes d'intelligence artificielle



Dans ce cas, une instruction complète du dossier est réalisée.

5.2.2 Instruction du dossier et audit documentaire par l'Organisme Certificateur

À réception du dossier de candidature, tel que défini ci-dessus, l'Organisme Certificateur procède à son examen avec pour finalité de s'assurer que les critères d'attribution de NFG (critères A et B) sont justifiés et que les risques liés à la non-conformité de la solution numérique sont maîtrisés, notamment en matière de souveraineté, de sécurité et de protection des données.

Le demandeur accepte d'être audité par l'Organisme Certificateur et de mettre à disposition de l'auditeur toute information ou document permettant de démontrer la conformité aux exigences du référentiel.

Le demandeur s'assure que ses prestataires, sous-traitants et fournisseurs intervenant dans la réalisation ou l'exploitation de la solution acceptent également d'être audités, et de mettre à disposition toute information nécessaire à l'évaluation des critères du référentiel.

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

Le demandeur s'assure contractuellement que ses prestataires et sous-traitants respectent les exigences du référentiel, notamment en matière de localisation, de sécurité, de protection des données et de transparence des opérations.

Maîtrise de la traçabilité et des flux numériques

L'Organisme Certificateur vérifie la pertinence et l'efficacité des dispositifs de traçabilité, de contrôle et de maîtrise décrits au point 5.2.1.4.

Examen du dossier

L'examen du dossier porte notamment sur les points suivants :

- La réception d'un dossier complet, conditionnant la poursuite de la procédure,
- La cohérence du périmètre déclaré (organisation, solution ou gamme de solutions),
- La cohérence de l'architecture de la solution et des étapes de sa production et exploitation,
- La localisation des activités clés et leur conformité aux exigences de souveraineté (critère A),
- La cohérence de la méthodologie utilisée pour déterminer la part de valeur réalisée en France (critère B),
- L'identification et la maîtrise des dépendances technologiques critiques,
- La conformité des conditions d'hébergement, de traitement et de protection des données,
- La pertinence des dispositifs de traçabilité, de sécurité et de contrôle interne,
- Les preuves documentaires fournies pour étayer le respect des critères.

Une attention particulière est portée aux éléments relatifs :

- À la gouvernance et à la juridiction applicable,
- À la maîtrise des risques liés aux législations extraterritoriales,
- Aux dispositifs de cybersécurité,
- Ainsi qu'à la gouvernance des systèmes d'intelligence artificielle, lorsque la solution en intègre.



Rapport d'audit documentaire et avis

L'examen du dossier de candidature donne lieu à la remise d'un rapport d'audit documentaire portant un avis sur le respect des exigences du référentiel et l'éligibilité au schéma de garantie.

Deux types d'avis sont possibles :

- **Conformité au référentiel** : le demandeur est éligible à l'attestation de conformité,
- **Non-conformité au référentiel** : le demandeur est non éligible en l'état à l'attestation de conformité.

Audit initial

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

L'audit initial est réalisé par un organisme tiers indépendant. Il comprend :

- Une vérification documentaire, telle que décrite ci-dessus,
- Et, le cas échéant, un audit sur site ou sur les environnements techniques, en fonction de l'analyse de risques réalisée par l'Organisme Certificateur.

Un délai de 6 à 8 semaines peut être observé entre la phase d'examen documentaire et la réalisation de l'audit initial.

L'Organisme Certificateur précise, sur la base de l'analyse du dossier :

- Les modalités de l'audit initial,
- Les lieux ou environnements audités,
- Les points sensibles nécessitant une vérification approfondie,
- Ainsi que les éventuels audits à prévoir chez les prestataires ou sous-traitants.

Organisation des audits complémentaires

L'Organisme Certificateur peut être amené à réaliser des audits complémentaires :

- Sur les sites du demandeur,
- Après de ses prestataires ou sous-traitants,
- Ou sur des environnements techniques (infrastructures, systèmes, outils).

Le demandeur a la responsabilité de garantir le bon déroulement de ces audits, notamment en facilitant l'accès :

- Aux sites,
- Aux systèmes d'information,
- Aux environnements techniques pertinents,
- Et aux documents nécessaires à l'évaluation.



5.2.3 Décision et délivrance de l'attestation

La décision de la délivrance de l'attestation de conformité est prise par l'Organisme Certificateur sur la base du rapport d'audit, des éventuelles non-conformités identifiées et de leur traitement, et de l'évaluation globale du respect des critères A et B. Lorsque la solution intègre des systèmes d'intelligence artificielle, la décision tient compte de leur niveau de maîtrise, de leur provenance et des dispositifs de prévention des biais et dérives.

L'attestation de conformité au référentiel Numérique France Garanti est délivrée pour la solution ou gamme de solutions concernée à l'issue de l'audit, sous réserve de conformité aux exigences du référentiel.

En cas de non-conformité, le demandeur dispose d'un délai défini pour mettre en œuvre des actions correctives. La délivrance de l'attestation est conditionnée à la levée de ces non-conformités.

5.2.4 Suivi de la démarche

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

L'attestation de conformité au référentiel NFG est délivrée pour une durée de trois ans, avec deux audits de surveillance annuels, afin de s'assurer du maintien de la conformité.

Les audits de surveillance visent à vérifier :

- Le maintien de la conformité aux critères A et B,
- L'absence d'évolution remettant en cause la souveraineté, la sécurité ou la localisation,
- La bonne application des mécanismes de contrôle, et
- La cohérence entre le périmètre évalué et la réalité opérationnelle.

Ils peuvent inclure une revue documentaire, des vérifications techniques, et le cas échéant, des audits ciblés.

5.2.5 Phase pilote et évolution du référentiel

Dans le cadre du lancement de Numérique France Garanti, une phase pilote est mise en œuvre.

Les entreprises participantes sont auditées sur la base de la version initiale du référentiel. Leurs retours permettent d'ajuster les exigences, notamment en matière de seuils, de modalités d'évaluation et de prise en compte des spécificités sectorielles.

À l'issue de cette phase, une version consolidée du référentiel est établie.

5.2.6 Suspension et retrait



L'entreprise ayant des solutions numériques Numérique France Garanti s'engage à :

- maintenir la conformité de la solution certifiée aux exigences du référentiel,
- mettre à disposition les éléments nécessaires aux audits de suivi,
- garantir la cohérence entre le périmètre certifié et les communications associées,
- informer les instances en charge de l'évaluation et de la démarche de toute modification susceptible d'affecter cette conformité.

En particulier, les titulaires de l'attestation de conformité doivent prévenir l'association Origine France Garantie et l'Organisme Certificateur en cas de :

- Rachat ou modification majeure de gouvernance,
- Faille de sécurité sur les données ou la chaîne de valeur
- Dérive d'une intelligence artificielle

En cas de non-conformité ou d'événement susceptible d'affecter la conformité au référentiel, des mesures de suspension ou de retrait de l'attestation peuvent être décidées lors du prochain Comité Technique de la Marque Numérique France Garanti.

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

Des audits complémentaires peuvent être réalisés afin d'évaluer la situation et statuer sur le maintien de l'attestation.

6. MODIFICATION ET EXTENSION DU PERIMETRE DE GARANTIE

L'attestation de conformité est délivrée sur la base d'un dossier initial de demande précisant un périmètre de solution numérique.

Le demandeur a pour obligation, sous peine de se voir suspendre l'usage de la Marque de Garantie, d'informer l'Organisme Certificateur agréé par l'association Origine France Garantie de toute modification mettant en cause les termes de l'attestation, les modifications du processus de mise en œuvre de la solution numérique ainsi que les intervenants impliqués dans le respect du référentiel.

Exemples :

Évolutions techniques de la solution : modification de l'architecture technique ou fonctionnelle, introduction de nouvelles fonctionnalités ou services, évolution des composants logiciels ou des dépendances critiques, modification des conditions d'hébergement ou de la localisation des données.

Évolutions opérationnelles : évolution significative des volumes traités ou des usages, modification des ressources humaines affectées aux activités clés, évolution des sites ou environnements techniques d'exploitation.

Évolutions de la chaîne de valeur et de la gouvernance : modification des modalités de sous-traitance ou des prestataires intervenants, introduction de nouveaux fournisseurs ou partenaires structurants, évolution de la gouvernance ou de l'actionnariat de l'organisation titulaire de l'attestation, modification du détenteur de l'attestation NFG.



A réception de ces informations, l'Organisme Certificateur agréé par l'association procède à sa propre analyse de risque et précise les modalités de modification ou d'extension de l'attestation et ainsi du droit d'usage de la Marque de Garantie.

Exemples : simple examen documentaire, audit spécifique sur site ou environnement technique, extension du champ de l'audit lors d'un audit de suivi programmé...

6.1 EVOLUTION DES REGLES DU RÉFÉRENTIEL

Lors de l'évolution d'une annexe, l'entreprise bénéficie pour se mettre en conformité avec la nouvelle règle : soit d'un délai prévu spécifiquement dans l'annexe concernée, soit de la durée restant jusqu'à la date d'échéance de l'attestation (au terme du contrat en cours).

6.2 AUDIT DE RENOUVELLEMENT DE L'ATTESTATION DE CONFORMITÉ APRÈS TROIS ANS

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

À la fin de la période des trois ans, l'entreprise doit demander le renouvellement de son attestation. Les solutions numériques concernées et leur processus de mise en œuvre étant déjà connues de la part des Organismes Certificateurs, la procédure de renouvellement est donc allégée. Seul un audit de renouvellement est nécessaire, procédure qui s'apparente à un audit de suivi où l'Organisme Certificateur réalise des contrôles et des vérifications sur les solutions numériques concernées.

La dernière version du référentiel est rendue applicable aux solutions en demande de renouvellement. L'audit de renouvellement doit avoir lieu avant expiration de l'attestation de conformité en vigueur afin de pouvoir émettre la nouvelle attestation avant l'échéance de la précédente.

Cette procédure de renouvellement est valable uniquement s'il n'y a pas de changement d'Organisme Certificateur de la part de l'entreprise concernée. Dans le cas contraire, celle-ci devra recommencer une procédure d'évaluation depuis le début avec le nouvel Organisme Certificateur qu'elle aura choisi.

Si une entreprise présente une non-conformité en audit de renouvellement, l'Organisme Certificateur lui indique qu'elle dispose d'un délai limité (6 mois) pour se mettre en conformité avec les critères du référentiel. Durant cette période, l'entreprise peut utiliser l'attestation de conformité et est éligible à la redevance de marque. S'il y a deux « non-conformités » consécutives, l'entreprise perd son attestation de conformité. Enfin, l'Organisme Certificateur avertit Origine France Garantie de cette situation dès qu'il en a l'information.

7. COMMUNICATION SUR L'OBTENTION DE LA GARANTIE

L'attribution de l'attestation de conformité confère au demandeur une concession d'usage à titre onéreux de la marque « Numérique France Garantie » pour la durée mentionnée dans le Règlement d'usage de la marque et selon les termes et conditions indiqués notamment dudit Règlement.

L'usage de la marque « Numérique France Garantie » doit scrupuleusement respecter la charte de communication de la Marque transmise par le Certificateur à l'entreprise.

Si une entreprise est couverte par une attestation portant uniquement sur certaines solutions numériques, la communication relative à « Numérique France Garantie » doit être strictement limitée à ces solutions. Lorsqu'une entreprise est couverte pour l'ensemble de ses solutions numériques entrant dans le périmètre, une communication globale peut être réalisée.

L'association Origine France Garantie valide tous les usages de marque afin de maîtriser la communication des entreprises concernant NFG et vérifier que le consommateur n'est pas induit en erreur. Ainsi le risque de communication erronée ou trompeuse est maîtrisé.

Conformément à l'article L.433-6 du code de la consommation « Toute référence à la certification dans la publicité, l'étiquetage ou la présentation de tout produit ou service, ainsi

	NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

que sur les documents commerciaux qui s'y rapportent est accompagnée d'informations claires permettant au consommateur ou à l'utilisateur d'avoir facilement accès aux caractéristiques certifiées. La consultation des référentiels de certification s'effectue soit gratuitement auprès de l'organisme certificateur, soit par la délivrance d'exemplaires aux frais du demandeur. »

8. DÉCLINAISONS GEOGRAPHIQUES

TERRITOIRE FRANÇAIS :

Le territoire français couvre tous les départements français, notamment les départements d'outre-mer, ainsi que les territoires d'outre-mer. Le schéma de garantie ne concerne pas les produits de Monaco.



REGLES DE DECLINAISON GEOGRAPHIQUE :

Une entreprise dont les solutions numériques sont « Numérique France Garanti » peut choisir de communiquer sur une zone géographique plus réduite que le territoire français dans la mesure où elle respecte les règles suivantes :

- Si le ou les lieux où la solution numérique prend ses caractéristiques essentielles se situent tous dans une région donnée, l'entreprise reçoit une attestation de conformité mentionnant précisément l'origine géographique. Elle peut décider de mettre en avant cette **région** en la nommant à côté du logo « Numérique France Garanti », conformément à la charte graphique.
- Si le ou les lieux où la solution numérique prend ses caractéristiques essentielles telles que définies dans le référentiel se situent tous dans un département donné, l'entreprise peut décider de mettre en avant ce **département** en le nommant sous le logo « Numérique France Garanti », conformément à la charte graphique.
- Si le ou les lieux où la solution numérique prend ses caractéristiques essentielles telles que définies dans le référentiel se situent tous dans une ville donnée, l'entreprise peut décider de mettre en avant cette **ville** en la nommant sous le logo « Numérique France Garanti », conformément à la charte graphique.
- Si les lieux où la solution numérique prend ses caractéristiques essentielles telles que définies dans le référentiel ne se situent pas tous dans une région donnée, l'entreprise ne peut pas mettre en avant de zones géographiques précises.

9. ANNEXES SECTORIELLES

La liste à jour des annexes est transmise aux Organismes Certificateurs. Se reporter à la liste en vigueur (cf. « Liste des référentiels applicables ») dans sa dernière version.

	<p>NUMÉRIQUE FRANCE GARANTI « Référentiel socle » de délivrance de la garantie</p>	Document	RS	
		Version	V5 projet	
		Date	00/00/2026	

HISTORIQUE DES EVOLUTIONS DU REFERENTIEL « NUMÉRIQUE FRANCE GARANTI » :

Résumé de la modification	Rédacteur/ice	N° Version Cible	Date de la Version
Création	M. JANICHON	V0 (projet)	24/04/2026