

Recommandations pour le partage de données par API¹ dans l'administration

Enjeux stratégiques et conseils opérationnels : produire et diffuser ses API²

Avril 2022

Pourquoi un cadre de recommandations pour le partage de données par API ?

Les données sont un actif stratégique pour la modernisation du service public et de l'action publique. Elles facilitent la mise en œuvre et le pilotage des politiques publiques, et leur circulation permet la simplification des démarches administratives pour les citoyens et les entreprises.³

Le cadre interministériel d'administration de la donnée, publié en septembre 2021, précise le cadre dans lequel les administrations doivent inscrire leur action en la matière. Il décrit également l'offre de service mise à leur disposition afin de concevoir et de mettre en œuvre à leur échelle, ainsi qu'à celle de leurs opérateurs, des stratégies ambitieuses en matière de données, d'algorithmes et de codes sources.

Le présent document précise ce cadre d'action et identifie les bonnes pratiques à poursuivre en matière d'usage et d'exposition d'API par les administrations.

Depuis l'adoption de la loi Différenciation, Décentralisation, Déconcentration et Simplification (dite loi 3DS), le code des relations entre le public et l'administration (CRPA) prévoit que : **« Les administrations échangent entre elles toutes les informations ou les données strictement nécessaires pour traiter une demande présentée par le public ou une déclaration transmise par celui-ci en application d'une disposition législative ou d'un acte réglementaire. (...) Les administrations peuvent échanger entre elles les informations ou les données strictement nécessaires pour informer les personnes sur leur droit au bénéfice éventuel d'une prestation ou d'un avantage prévus par des dispositions législatives ou des actes réglementaires et pour leur attribuer éventuellement lesdits prestations ou avantages. »**

¹ Applicative Protocol Interface ou interface de programmation: dispositif informatique permettant l'échange d'informations entre deux ordinateurs (<https://api.gouv.fr/guides/api-definition>).

² Ce document concerne les API d'accès en lecture ou écriture sur des ressources en données (ex : OGC API, OpenAPI...) et non les API qui apportent un service sur des données (ex : horodatage).

³ Le cadre juridique applicable pour l'échange de données par API est défini dans le code des relations entre le public et l'administration (CRPA) et le Règlement général de protection des données (RGPD)

Cette promulgation de la loi 3DS va donc induire une accélération forte du nombre de raccords aux API. En outre, la charte signée avec les collectivités territoriales⁴ pour le déploiement de FranceConnect et des API va contribuer à cette accélération.

Les données gérées par l'administration doivent donc circuler rapidement et facilement entre les producteurs et les réutilisateurs, dans le respect de leur besoin de protection.

Différents types d'API permettent de partager ces données et facilitent leur circulation, notamment entre les administrations.

Cette note propose des orientations pour le développement d'API ouvertes ou en accès restreint. Elle traite des API visibles et accessibles sur un portail web. Ces principes formulés ci-après ont été définis par un ensemble d'administrations à la suite d'une concertation orchestrée par la DINUM dans la continuité de la publication du cadre interministériel d'administration des données.

6 enjeux stratégiques

6 enjeux stratégiques ont été identifiés afin de répondre au mieux aux besoins des utilisateurs, qu'il s'agisse d'administrations ou d'utilisateurs, tout en s'intéressant à la gestion du service proposé.

1. Découvrabilité
2. Accès à la donnée
3. Exploitation des données
4. Qualité de service
5. Curation de la donnée
6. Modèle économique

⁴ https://www.numerique.gouv.fr/uploads/Charte_engagement_FranceConnect-API.pdf

1. Découvrabilité

Catalogue de données et services disponibles

Recommandation 1

En complément de la description (métadonnées), les données et services publiquement accessibles sont visibles sur un catalogue exposé sur Internet, référencé sur les moteurs de recherche usuels et intelligibles (la description des API au sein du catalogue ou de l'API manager propose un contenu destiné aux opérationnels, fonctionnels comme techniques).

La description d'une donnée doit référencer les API qui l'exposent. L'exemple présenté ci-dessous met ainsi en évidence les ressources accessibles sur la page présentant le jeu de données « base SIREN des entreprises et de leurs établissements ».

Les APIs de api.gouv.fr pour ce jeu de données

	API Conventions collectives Retrouvez les conventions collectives d'une entreprise à partir de son numéro SIRET	Ministère du Travail, de l'Emploi et de l'Insertion
	API Sirene données ouvertes Accéder librement aux informations des entreprises et des établissements de la base Sirene	Direction Interministérielle du Numérique
	API Sirene Accéder aux informations concernant les entreprises et les établissements immatriculés au répertoire interadministratif Sirene de l'Insee	Institut national de la statistique et des études économiques

Exemples :

- *api.gouv.fr* vise à référencer toutes les API publiques de l'Etat
- API Impôt Particulier vise à référencer la donnée fiscale des particuliers

Recommandation 2

À chaque API exposée correspond :

- Une documentation fonctionnelle présentant la sémantique des données, leur qualité ainsi que leur source et leurs propriétés usuelles. Elle explicite également le processus de demande d'accès et l'éligibilité des réutilisateurs. Si un catalogue existe, un lien vers la description de la donnée est proposé ;
- Une documentation technique présentant les modalités d'interrogation et de

récupération de la donnée ;

- Les conditions générales d'utilisation précisant les conditions contractuelles d'accès à l'API.

La spécification d'une API respecte les standards répandus au sein de la communauté (norme OpenAPI en 2022). Cette description ne doit pas doubler avec celle d'une donnée existante, ni ne s'affranchit de la nécessité de décrire la donnée dans un catalogue de donnée (principe de découvrabilité). Une API fournissant plusieurs jeux de données doit être décrite une seule fois et intégrer les liens vers chaque description des données fournies.

La description d'une API précise également les périodes de validité de l'interface (cf. recommandations 7 & 8) et son niveau de service (cf. recommandations 10 & 11).

Accès à la donnée

Gestion des habilitations d'accès aux API à accès restreint

Recommandation 3

L'accès aux API à accès restreint se fait par demande du réutilisateur (administrations, éditeurs, entreprises...).

Les API peuvent s'appuyer sur un mécanisme d'authentification de l'utilisateur final assurant une gestion des droits au sein de la plateforme qui les fournit. Les dispositifs d'authentification des citoyens, des agents ou des personnes morales conçus par les pouvoirs publics pourront être utilisés, en particulier lorsque le consentement de l'utilisateur est nécessaire pour faire circuler la donnée :

- Pour les personnes physiques : FranceConnect, AgentConnect et EduConnect
- Pour les personnes morales : ProConnect

Recommandation 4

Si le droit d'accès n'est pas préétabli, le processus de demande se fait de la manière la plus simple possible pour le réutilisateur. Dans le cadre de demandes d'accès prévues par la loi et si le demandeur est éligible, une réponse sera transmise aux réutilisateurs dans un délai

recommandé de 15 jours calendaires. Le code des relations entre le public et l'administration prévoit un délai légal maximum de 30 jours pour répondre à une demande (article R311-13).

Bac à sable d'expérimentation public

Recommandation 5

À chaque API devrait correspondre une version « bac à sable », accessible en fonction du caractère des données ouvertes ou en accès restreint, exposant une version fictive des données et présentant les mêmes modalités techniques d'exposition.

Pour les API ouvertes, le bac à sable potentiel est accessible au grand public, sans demande préalable du réutilisateur. Pour les API à accès restreint, le bac à sable contenant des données fictives pourrait être accessible au réutilisateur après demande d'un jeton au fournisseur de données, bien que cette pratique ne soit pas recommandée.

Exploitation des données

Utilisation des standards technologiques du moment pour faciliter l'interopérabilité

Recommandation 6

Les données et services sont exposés selon des standards techniques communément partagés et adoptés.

En 2022, le principe d'architecture et d'encodage le plus connu et pratiqué est le standard REST Json pour les API synchrones. Il est utilisé par exemple pour les spécifications du standard OpenAPI (<https://spec.openapis.org/oas/v3.1.0>) ou les standards « API » de l'OGC (<https://ogcapi.ogc.org>). Concernant les API asynchrones, le principe AsyncAPI est le plus répandu.

👍 **Bonne pratique** : L'approche « contract first », par opposition à l'approche « code first », est recommandée dans le développement de nouvelles interfaces car elle permet de les stabiliser et de faire travailler plusieurs équipes en parallèle au sein d'une même architecture.

Stabilité du modèle des interfaces

Recommandation 7

Les données et services sont exposés selon une interface (modalités d'appel et structuration des données échangées) définie pour une période donnée.

Les développements Agile ou nécessitant une évolution prévisible seront rendus identifiables et préciseront une période de validité courte de 1 à 2 mois.

Recommandation 8

Ces périodes de validité de l'interface sont explicitement présentées aux réutilisateurs dans la documentation. Les modifications prévisibles s'accompagneront de l'actualisation préalable des informations descriptives intégrant des liens vers des communications et guides permettant aux réutilisateurs d'anticiper les évolutions. Les réutilisateurs pourront basculer durant une période définie et communiquée sur la version modifiée de l'interface. Durant ce laps de temps, deux interfaces cohabiteront, la version précédente dépréciée et la nouvelle version.

Le détail de ces informations sera présenté en détail dans les conditions générales d'utilisation de l'API.

Recommandation 9

Toute modification non rétro-compatible impose un versioning en tant que version majeure et une cohabitation de l'ancien et du nouveau modèle pendant une période de recouvrement. Celle-ci doit être communiquée à l'avance en diffusant le nouveau contrat d'interface de l'API. À défaut d'information préalable ou d'accord des réutilisateurs, la période de cohabitation sera comprise entre 6 mois et 1 an.

Si une évolution de la donnée interdit le maintien de l'ensemble des fonctionnalités de l'API (exemple : modification d'un schéma avec abandon de certaines informations), il sera indiqué quelles requêtes ou parties du protocole seront maintenues.

Qualité de service

Indications sur le temps de réponse et la tenue en charge

Recommandation 10

La charge admise par une API est consultable en toute transparence par les réutilisateurs :

- Dans le cas d'une API authentifiée, la charge est exprimée sous forme de métriques propres à chaque réutilisateur, comme le nombre d'appels sur une période donnée par exemple ;
- Dans le cas d'une API non authentifiée, la charge tenable est exprimée dans son ensemble, tous réutilisateurs confondus ;
- Dans le cas d'une infrastructure permettant, via une API, des requêtes complexes, ou servant de nombreuses données, la charge tenable estimée indiquera les critères utilisés et le caractère estimatif de cette évaluation ;
- Dans le cas d'une API sujette à des fortes évolutions en fonction de la saisonnalité, le temps de réponse maximal sera précisé ainsi que les risques de rupture de service.

Recommandation 11

Les temps de réponse moyens et maximaux sont présentés dans la documentation de l'API. Les temps de réponse mesurés ou estimés sont fournis à titre indicatif et non contractuel. Tout autre démarche relève d'un d'accord entre le fournisseur d'API et les réutilisateurs en fonction de leurs cas d'usages.

Transparence sur la disponibilité de l'API

Recommandation 12

L'état de l'API représente sa capacité à être appelée dans les conditions réelles par un réutilisateur. Il est rendu accessible aux réutilisateurs et consultable en temps réel sous forme d'une URL, indiquée dans la description de l'API, permettant de tester que l'API se déclare disponible et requetable. En complément, il est souhaitable de permettre de consulter un historique entre 6 mois et une année.

Exemple :

Le suivi de la disponibilité des API du bouquet API Entreprise est disponible au lien suivant : <https://status.entreprise.api.gouv.fr/>

Suivi des consommations des données et services

Recommandation 13

Les consommations des API sont enregistrées pour être ensuite restituées aux bénéficiaires (réutilisateur, producteur, API managers ou exploitants).

👍 **Bonne pratique** : les bénéficiaires ont accès à travers un portail à une restitution en temps réel ou ponctuelle de ces statistiques de consommation des données ainsi que celles des autres bénéficiaires.

Curation de la donnée

Mise en place d'une boucle de retour sur la qualité des données

Recommandation 14

Les réutilisateurs disposent d'un moyen technique ou organisationnel leur permettant de faire des retours sur la qualité des données vers leur gestionnaire ou via la description des données au sein de leur catalogue d'origine. Les réutilisateurs disposent également d'un moyen technique ou organisationnel leur permettant de faire des retours sur la qualité des API exposées vers leur fournisseur ou via la description de l'API.

Exemple :

Le dispositif Datapass pouvant être utilisé par les API en accès restreint permet de faire un retour sur la qualité des données disponibles via celles-ci.

Modèle économique

Gratuité de la donnée et de l'exposition

Recommandation 15

L'accès à la donnée et aux services doit être égalitaire. Les fournisseurs de données cherchent à adapter les modalités d'accès aux besoins des réutilisateurs.

Recommandation 16

Les données ainsi que les API sont mises à disposition gratuitement, pour les réutilisateurs uniquement, sauf exceptions devant faire l'objet d'une justification par l'administration productrice.

Exemple :

Dans le cas où des usages nécessiteraient une qualité de service au-dessus de ce que la multitude d'utilisateurs a couramment besoin, comme par exemple une bande passante élevée pour de la donnée temps-réel volumineuse desservie sur quelques organismes, il sera possible d'organiser un système freemium avec une égalité d'accès à des APIs par défaut et des APIs faisant l'objet de redevances pour les usages les plus exigeants.