Politique de contribution aux logiciels libres de l'État v1.0

Direction interministérielle du numérique et du système d'information et de communication de l'État

18 mai 2018

Historique et versions

Version	Commentaire	Date
0.1	Initialisation	01/11/2017
0.2	Ouverture de l'appel à commentaires	06/12/2017
0.3	Fin de l'appel à commentaires	28/01/2018
1.0RC01	Projet soumi à validation	10/02/2018
1.0	Validation en CSIC Tech	16/02/2018

Table des matières

Introduction

Objectifs

Conformément à la Loi pour une République numérique du 7 octobre 2016, les codes sources sont des documents administratifs communicables et réutilisables. Dans le cas où il est possible de choisir une licence libre, le décret n° 2017-638 du 27 avril 2017 précise les familles de licences qui peuvent être utilisées. La liste détaillée des licences avec leurs versions est disponible sur le site data.gouv.fr.

Les objectifs de cette politique interministérielle de contribution aux logiciels libres sont de :

- fixer les règles et principes à respecter pour l'ouverture des codes sources
- accompagner les ministères et partager les bonnes pratiques
- définir la gouvernance des politiques de contribution de l'État.

Ce document est à destination des développeurs ou de leurs responsables, qu'ils soient agents publics (titulaires ou contractuels) ou prestataires.

Périmètre

Cette politique de contribution s'applique au système d'information et de communication de l'État conformément à l'article 1er du décret n° 2014-879 du 1er août 2014. Chaque administration de l'État a la possibilité d'instancier sa propre politique de contribution pour la préciser et l'amender.

Sont concernés l'ensemble des codes sources :

- développés en interne par l'administration
- développés pour le compte de l'administration.

Cette politique de contribution vise les *nouveaux* développements afin qu'ils respectent les bonnes pratiques. Pour l'ouverture de codes sources existants, des actions complémentaires seront nécessaires, telles que la définition du périmètre d'ouverture du code, sa revue qualité, sa revue sécurité, l'analyse de conformité et l'analyse de la propriété intellectuelle.

Les fonctions publiques hospitalières et territoriales sont hors périmètre de cette politique de contribution mais elles peuvent s'en inspirer librement.

Structure du document

La politique de contribution est composée de :

- Principes d'ouverture des codes sources
- Modalités et bonnes pratiques
- Instanciation de politique de contribution ministérielle
- Gouvernance associée

Responsabilité du document

La DINSIC produit et maintient ce document ; elle veille à sa mise en œuvre et assure le support associé. Pour toute question, ou demande d'évolutions, veuillez vous référer à la partie *Gouvernance*.

Références externes

Ce document a été élaboré grâce aux nombreux travaux ci-dessous :

- Open Government Partnership collaboration
- USA 18F Open Source Policy
- Whitehouse Source Code Policy
- UK GDS (Governement Digital Service)
- Canada British Columbia
- Australia Digital Transformation Agency
- Linux Foundation Open Source Guides
- Core Infrastructure Initiative
- Open Source Guides
- FSFE software reuse
- Google Open Source

Un travail est également en cours par le gouvernement du Canada : Open First Whitepaper.

Principes d'ouverture des codes sources

Préambule

Principe de subsidiarité

La politique peut être instanciée localement avec une priorité plus forte.

Voir la section instanciation si vous souhaitez décliner cette politique au sein de votre organisation.

Assistance sur la politique de contribution

Contacter `opensource @ data.gouv.fr` pour toute question sur cette politique.

Principe de reconnaissance des contributions

Attribuer les contributions aux individus

Afin de reconnaître la paternité des contributions, l'adresse électronique individuelle du développeur est utilisée:

- Pour les agents : utilisation de l'adresse électronique professionnelle.
- Pour les prestataires de services, utilisation de l'adresse électronique de leur société d'attachement (pas d'adresse prestataire fournie par l'administration)

Toutefois, au cas où un développeur ne souhaiterait pas voir son identité publiée, il peut utiliser un pseudonyme. En revanche, l'utilisation d'adresses électroniques génériques ou anonymes est à

proscrire.

Distinguer les contributions professionnelles et personnelles

Il est possible pour un développeur de contribuer sur un même projet dans le cadre du milieu professionnel et à titre personnel, l'État reconnaissant aux développeurs la propriété sur les contributions réalisées en dehors du temps de travail. Les contributions réalisées sur le temps professionnel doivent être associées à une adresse électronique professionnelle.

Contribuer à des projets tiers

Autorisation par défaut de contribuer à des projets sous licence FSF ou OSI

Les licences validées par les organismes Free Software Foundation et Open Source Initiative et recensées sur leurs pages respectives :

- FSF : https://www.gnu.org/licenses/license-list.fr.html (en excluant les licences non libres présentées comme telles) ;
- OSI : https://opensource.org/licenses/alphabetical.

À l'inverse les licences non retenues par ces organismes (comme la *Beerware*) ne rentrent pas dans le cadre de l'autorisation par défaut. Un tableau consolidé des licences validées par l'un ou l'autre organisme est maintenu sur le site https://spdx.org/licenses/

Signature des *Corporate Contributor License Agreement*

La DINSIC prend en charge de signer les accords de contributions spécifiques (Corporate Contributor License Agreement ou CCLA) avec les communautés ou les entreprises qui l'exigent, afin de permettre les contributions des agents à titre professionnel aux projets concernés. Si cela est demandé par l'autre partie, elle maintiendra les listes d'individus couverts par l'accord. Une autre possibilité est que l'accord de CCLA soit un pré-requis à la signature d'un Contributor License Agreement individuel (iCLA). Dans ce cas, la signature d'un CCLA par la DINSIC vaudra pré-autorisaiton pour la signature d'iCLA.

Si vous souhaitez contribuer à un projet réclamant ce type de formalisme, que ce soit pour signer un CCLA, vous rajouter à la liste des contributeurs autorisés, ou vérifier la possibilité de signer un iCLA, contactez l'adresse d'assistance indiquée plus haut.

Liste des CCLA signés:

- A ce stade, aucun CCLA n'a encore été signé par la DINSIC.

Contribuer en publiant un nouveau projet

La publication du code source ne crée ni obligation ni garantie

- Aucune obligation de support et de prise en compte des demandes des utilisateurs ni plus généralement d'obligation d'animer la communauté.
- Pas de garanties au-delà de ce qui est prévu par la licence.

Autorisation par défaut de contribuer un nouveau projet avec les licences du décret

L'État n'a pas vocation à être éditeur de logiciels. En dehors des trois exceptions prévues à la loi pour une République numérique pour lesquelles vous pouvez contacter l'adresse électronique de support en cas de question, il n'y a pas d'autorisation préalable à demander auprès de la DINSIC. Pour autant, veuillez vous référer à votre supérieur hiérarchique avant la publication d'un nouveau projet dans le compte de votre organisation.

Pour rappel, les licences à utiliser sont disponibles par décret sur le site : http://www.data.gouv.fr/fr/licences.

Éléments à considérer dans le choix de la licence libre

Pour les cas où l'administration a des raisons de garantir que les modifications apportées par un tiers au logiciel libre qu'elle publie sont accessibles sous les mêmes conditions, elle envisagera une licence à réciprocité. En particulier, s'il s'agit d'un logiciel qui est à la base d'un service en ligne pour lequel elle souhaite se prémunir de toute réappropriation, elle pourra considérer la licence GNU Affero General Public License. Dans les autres cas, elle considérera les licences permissives.

Le choix de la licence d'un projet devra également prendre en compte celles des composants Open Source tiers constituant son cadre technique, selon les modalités de leurs relations techniques.

L'écosystème où s'insère le projet pourra aussi aiguiller le choix de la licence, dans la limite de la latitude laissée par les critères précédents.

À noter que les solutions logicielles sont souvent modulaires et que la question de la licence peut se poser à plusieurs niveaux. Par exemple, pour une solution de site web, les modules de l'interface web pourront être publiés sous une licence différente de celle qui couvre le code source côté serveur.

Certification de l'origine des contributions (DCO)

Les projets publiés par l'État n'exigent pas de droits spécifiques des contributeurs en dehors de ceux accordés par leurs licences respectives (pas d'utilisation de CLA). En revanche, il est demandé aux contributeurs de signer un Certificat d'origine des contributions (*Developer Certificate of Origin*). Afin de s'insérer dans les standards en usage, il a été choisi d'utiliser une traduction française du texte utilisé pour le noyau Linux et repris par de nombreux autres projets.

Bonnes pratiques

Système de suivi de version de code source

L'utilisation d'un système de suivi de version distribué tel que git est recommandée. Les systèmes svn ou cvs sont déconseillés.

Aide au choix d'une plateforme Web

En plus du système de suivi de version du code source, une plateforme Web propose une panoplie d'outils collaboratifs associés et vise à mobiliser une communauté de développeurs. Ces plateformes peuvent être hébergées par un tiers ou par l'administration.

Exemples de plateformes Web hébergées par un tiers :

- Github : https://github.com
- Gitlab : http://gitlab.com (version entreprise)
- Framagit : http://framagit.org - utilisant Gitlab
- Adullact : http://gitlab.adullact.net - utilisant Gitlab
- FSFE : https://git.fsfe.org - utilisant Gitea
- FSF : https://git.savannah.gnu.org/cgit/ - utilisant cgit

Le code source de github.com n'est pas libre tout comme certains modules de gitlab.com ; certaines plateformes publient des données anonymisées en open data ; leurs portées géographiques peuvent varier, de même que le nombre de développeurs qui l'utilisent. La liste est incomplète.

Le choix de créer un compte d'organisation au sein d'une plateforme Web existante relève de l'administration, qui peut également héberger sa propre forge publique.

Le positionnement d'un projet sur une forge doit se faire en fonction du niveau de collaboration attendu et des interfaces avec les dépots privés et le reste de la plateforme de développement.

Gestion des comptes personnels et d'organisation

Tous les projets initiés par une administration doivent être publiés dans des dépôts au sein de comptes d'organisation. Les dépôts de comptes personnels ne doivent être utilisés que pour des fourches (*forks*) techniques temporaires ou des développements personnels.

Il est recommandé d'avoir deux propriétaires par dépôt.

Inventaire des comptes d'organisation

Des réflexions sont en cours sur la capacité de proposer un inventaire automatique tant du point de vue des dépôts d'organisation que de l'inventaire des services.

> Pour référencer le compte d'organisation comme un compte gouvernemental dans Github :
>
> - Inscrivez vous si ce n'est pas déjà fait dans la communauté https://github.com/government/welcome
> - Référencez votre compte d'organisation en l'ajoutant sur la page : https://github.com/github/government.github.com/blob/gh-pages/_data/governments.yml conformément à la page https://government.github.com/community/

Distinction des contributions personnelles / professionnelles

La distinction entre contributions personnelles et professionnelles se base sur l'adresse électronique associée. Le contributeur doit donc changer celle-ci en fonction de la situation où il se trouve. Dans le cas de l'utilisation de `git`, cela peut se faire simplement :

- Pour une contribution professionnelle : `git config user.email <prenom.nom@ministere.gouv.fr>`
- Pour une contribution personnelle : `git config user.email`

`<email@perso.fr>`

Pour connaître l'adresse électronique actuellement utilisée : `git config --get user.email`

Dans les cas où le contributeur ne souhaite pas voir son identité personnelle attachée à sa contribution, une adresse électronique (ou alias) devra être mise à disposition par le ministère pour permettre l'utilisation d'un pseudonyme. Attention certains projets open source peuvent refuser les contributions sous pseudonyme.

Aide au choix de la licence

Le choix d'une licence est aussi le choix d'une communauté de développeurs et d'un écosystème d'outils associés. Une fois la famille de licence trouvée, c'est avant tout la communauté visée qui détermine le choix.

Les licences recommandées par défaut sont :

- Permissive : Apache 2.0
- Avec obligation de réciprocité : GNU GPL v3 (standard, lesser ou affero en fonction)

  Multilicensing : il est possible de fournir un logiciel sous plusieurs licenses simultanément, bien que cela puisse entraîner de la confusion.

Gestion des versions

Avoir une politique de gestion des versions est recommandé. Le guide de versioning sémantique (https://semver.org/lang/fr/) est un bon exemple à suivre.

Fichiers présents dans le dépôt

Assurez-vous d'avoir au minimum les fichiers README, CONTRIBUTING et LICENSE.

- README : description du projet. Peut décrire l'objectif et l'administration à l'origine de la publication.
- CONTRIBUTING : guide de contribution, comment s'impliquer et identification du processus de contribution et des licences associées. Exemple: https://github.com/moby/moby/blob/master/CONTRIBUTING.md
- LICENSE : licence de publication du logiciel.
- MAINTAINERS : liste des mainteneurs du projet (avec des droits de vote ou de commit généralement). Exemple: https://github.com/moby/moby/blob/master/MAINTAINERS
- ROADMAP : feuille de route publique.
- CONDUCT : un code de conduite pour réguler la communauté de contributeurs. Des exemples peuvent être trouvés : https://www.djangoproject.com/conduct/ et https://github.com/18F/code-of-conduct.
- GOVERNANCE : décrit la gouvernance du projet, les rôles et les drois de votes. Un exemple est disponible dans ce dépôt le fichier `gouvernance.md`.
- NFR : choix d'architecture technique du projet qui ne correspondent pas à des exigences fonctionnelles.

Ces fichiers doivent être en texte simple ou avec du marquage minimum (ie Markdown). Il n'est pas recommandé d'utiliser des formats binaires (ie PDF)

Entête des fichiers sources

Conformément aux recommandations détaillées dans https://reuse.software chaque fichier de code source doit disposer de son auteur, de son identifiant de licence SPDX, ainsi que d'une copie de la licence dans le repository local.

- Exemples d'entête de fichier (headers) :

```
/*
* Copyright (c) 2017 Alice Commit <alice@example.com>
*
* SPDX-License-Identifier: BSD-2-Clause
* License-Filename: LICENSES/BSD-2-Clause_Alice.txt
*/
```

ou dans le cas d'un projet faisant un suivi automatique de ses contributeurs :

```
/*
* This file is part of project X. It's copyrighted by the contributors
* recorded in the version control history of the file, available from
* its original location http://git.example.com/X/filename.c
*
* SPDX-License-Identifier: BSD-2-Clause
* License-Filename: LICENSES/BSD-2-Clause_Charlie.txt
*/
```

Ces identifiants permettent de générer automatiquement des inventaires des licences sous la forme de « Bill of Material », afin de garantir la conformité du logiciel.

L'ensemble des identifiants SPDX est disponible à cette adresse : https://spdx.org/licenses/

Traçabilité des developpements (DCO)

Afin de garantir l'origine des contributions soumises, la mise en œuvre d'un Developer's Certificate of Origin est recommandée. Une traduction française est mise à disposition DCO-Fr.txt

Pour l'instant, le sign-off ne se fait qu'en anglais en utilisant la commande

```
git commit --signoff
```

Bonnes pratiques de développement

Les bonnes pratiques de développement courantes s'appliquent également en contexte de développement ouvert, et notamment celles liées au respect des référentiels en vigueur dans l'administration :

- Référentiel général d'interopérabilité (RGI)
- Référentiel général d'accessibilité pour les administrations (RGAA)
- Référentiel général de sécurité (RGS)

L'ouverture du code vient par ailleurs amplifier l'importance de certaines de ces bonnes pratiques :

- **Documentation**, à l'intérieur du code (commentaires et messages de *commit*) et hors du code.

- **Conformité juridique** dans l'utilisation de bibliothèques tierces. La très grande majorité des développements actuels reposant sur des bibliothèques Open Source tierces, il est nécessaire de s'assurer de la compatibilité de leurs licences respectives et du respect des obligations de celles-ci.
- **Modularisation des développements** afin de maximiser la réutilisation de code mais aussi d'isoler les éventuelles sources d'erreur
- **Respect d'une unique convention de développement** par projet.

Sécurité

Interlocuteur identifié

Il est recommandé d'identifier un responsable de la sécurité du projet qui sera garant de vérifier le respect des bonnes pratiques mises en œuvre durant le développement, et de traiter les éventuels incidents de sécurité. Il est également préférable d'avoir recours à une adresse électronique dédiée, à destination du responsable identifié au moins, pour traiter des incidents de sécurité ou des problèmes liés à la propriété intellectuelle qui seraient découverts par un tiers.

Développement sécurisé

- Écrire du code qui respecte des pratiques de sécurité reconnues et qui ne fait pas usage de constructions dangereuses dans le langage utilisé
  - SEI CERT Coding Standards
  - PHP The Right Way
  - Secure Coding Guidelines for Java SE
  - Importance des langages pour la sécurité
  - Sécurité et langage Java
  - Sécurité et langages fonctionnels
- Éliminer tous les messages de *debug* (par compilation conditionnelle ou par un contrôle via une variable à l'exécution) et toute information inutile pour l'utilisateur dans les messages d'erreur (e.g. trace d'appel Java/PHP/Python) lors de la mise en production
- Éliminer tout le code mort (*i.e.* code non appelé/non atteignable) car il pourrait prêter à confusion et/ou laisser penser qu'il est toujours fonctionnel et testé ; ce code, non maintenu, pourrait être réintégré à tort par un développeur
- Toutes les entrées externes (e.g. de l'utilisateur) doivent être contrôlées avant leur utilisation ou leur stockage, selon les bonnes pratiques de sécurité en fonction de leur destination.

Ne pas compter sur la sécurité par l'obscurité

La sécurité par l'obscurité est globalement reconnue comme une pratique insuffisante, mais dans le cas d'un projet dont le code est ouvert, cette stratégie est caduque. Elle doit donc être remplacée par d'autres stratégies plus robustes comme par exemple la défense en profondeur.

Données secrètes/sensibles, cryptographie

- Aucun élément secret (tel qu'un mot de passe ou une clé cryptographique) ne doit être stocké dans le code ou dans les commentaires; avoir recours à des fichiers de configuration qui ne sont pas versionnés (*cf* `.gitignore`)
- Aucun élément secret ne doit être écrit par le programme en clair dans un fichier (y compris un fichier de journalisation) ou dans une base de données, toujours préférer une version hachée par une fonction de hachage reconnue à l'état de l'art et correctement utilisée (*i.e* salée pour chaque entrée)
  - Référentiel général de sécurité - Annexe B3
- Aucun élément secret ne doit transiter en clair sur le réseau
- Ne pas implémenter soi-même de mécanisme cryptographique mais utiliser des bibliothèques reconnues en utilisant des paramètres et des suites cryptographiques robustes
  - Recommandations de sécurité relatives à TLS
  - Référentiel général de sécurité - Annexe B3

Outils de développement et dépendances

- Utiliser, le cas échéant, des logiciels et des bibliothèques tierces maintenus et à jour des correctifs sécurité; préférer des bibliothèques (re)connues, et les plus simples possibles
- Utiliser les services d'analyse de code offerts par la plateforme d'hébergement et traiter systématiquement avant intégration les problèmes remontés
- Ne pousser que des *commits* de code qui compilent, testés et fonctionnels, accompagnés des tests unitaires correspondants ; certaines plateformes offrent la possibilité de rejouer automatiquement les tests unitaires d'un projet afin d'assurer la non-régression (e.g Travis, Homu)
- Créer un *tag* (e.g. v2.0.1) pour chaque version (e.g. 2.0.1), et le signer cryptographiquement (voir GPG signature verification)
- Respecter les recommandations et bonnes pratiques de sécurité émises par l'ANSSI applicables au projet
  - Bonnes pratiques de l'ANSSI
  - Guide de sécurité méthodologie agile ANSSI / DINSIC

Outillage

La politique de contribution n'a pas vocation à proposer un outillage particulier. Toutefois spécifiquement pour la gestion de code ouvert, vous pourrez trouver les outils référencés sur https://www.linuxfoundation.org/tools-managing-open-source-programs/#1 utiles.

Instanciation des politiques de contribution ministérielles

En résumé

- Possibilité d'instancier et de reprendre cette politique
- Contacter la politique « mère » pour informer de la déclinaison

- Fournir obligatoirement un moyen de contact pour la politique instanciée

Inventaires des politiques ministérielles instanciées

- Aucune politique ministérielle instanciée à ce jour
- Exemple : <Ministère XXX> : http://reference.url/politique-ministerielle

Procédure d'instanciation

1. Fourcher ce dépot pour initier votre politique ministérielle
2. Faire une pull request sur ce fichier pour lister la politique de contribution fille et son URL
3. Contacter le support de cette politique et valider le moyen de contact principal de la politique fille

N'hésitez pas à prendre contact avec nous pour toute question.

Gouvernance de la politique de contribution interministérielle

La DINSIC maintient ce document et en est responsable (elle est propriétaire du dépôt et de la gestion des droits d'écriture). L'élaboration de cette politique a vocation à être collaborative et les entités auxquelles elle s'applique sont toutes invitées à participer à son évolution.

Deux types d'organisations sont distinguées :

- Interministériel : DINSIC et ANSSI
- Ministèriel

avec un seul rôle par organisation (droit d'écriture sur cette politique). L'ensemble des contributeurs avec les droits d'écriture sont listés dans le fichier MAINTAINERS.

Gestion des contributions

Toutes les contributions sont les bienvenues. Elles sont faites via une *pull request* sur la branche `next` qui est la branche d'élaboration d'une nouvelle version de la politique.

- les `pull request` apportant des modifications **majeures** doivent être approuvées par au moins trois organisations ministérielles et l'ANSSI.
- les `pull request` apportant des modifications **mineures** doivent être approuvées par au moins une organisation ministérielle.

Tous les mainteneurs ont la possibilité de fusionnner les *pull requests* sur la branche `next`. Si plusieurs mainteneurs appartiennent à un même ministère, leur validation ne compte que pour une organisation.

Gestion des versions

Seules la DINSIC et l'ANSSI peuvent fusionner sur la branche =master=qui correspond à la version validée :

- A chaque fusion sur la branche `master=un tag est ajouté suivant le schéma =v[MAJEUR].[MINEUR]` en fonction des *pull requests* approuvées sur la branche `next`.

- La politique de contribution open source peut être modifiée pour des changements légers (coquilles, etc.) sans mise à jour version (les numéros de PATCH de semver sont ignorés) directement sur la branche `master`.

Toutes les modifications peuvent être faites au fil de l'eau. Les discussions et commentaires sont tracées dans les commentaires de la *pull request*.

Foire aux questions

Périmètre

"Suis-je concerné(e) par cette politique de contribution open source ?"

Comme indiqué dans l'introduction, si la loi République Numérique s'applique à toute l'administration, le périmètre de la DINSIC se concentre sur la fonction publique d'État (avec quelques exceptions selon le décret n° 2014-879 du 1er août 2014).

Si vous faites partie d'une collectivité territoriale, cette politique ne vous concerne pas, bien que la loi République Numérique s'applique.

Si vous faites partie d'un opérateur ou d'un établissement public sous la tutelle d'un ministère, vous êtes concerné.

- et si j'appartiens à un établissement de recherche ?

  La loi République Numérique s'applique de la même manière.

- et si je suis salarié d'une ESN / SSII ?

  Si vous intervenez dans le cadre d'un marché public, vous êtes concernés. Toutefois, le détail des obligations contractuelles dépendra du CCTP et du CCAP.

- et si je suis indépendant / auto-entrepreneur ?

  Si vous travaillez pour une administration relevant du périmètre de la DINSIC, vous êtes également concerné.

"Quels sont les codes qui ont vocation à être ouverts ?"

L'obligation d'ouverture des codes est liée à la loi République Numérique qui prévoit une ouverture progressive jusqu'au 7 octobre 2018. A cette date, une ouverture par défaut est prévue pour tous les codes qui revêtent un intérêt économique, social, sanitaire ou environnemental.

Tout code écrit dans le cadre d'une mission de service publique est potentiellement communicable et réutilisable à d'autres fins, aux exceptions suivantes près :

- Le code doit être achevé (i.e. mis en production)
- Sa communication ne doit pas porter atteinte à :
  - Un secret protégé par la loi (secret commercial ou industriel d'un tiers, etc.)
  - La sûreté de l'État, la sécurité publique, des personnes ou des systèmes d'information des administrations
  - La recherche ou la prévention d'infractions de toute nature

"J'ai un doute sur l'ouverture d'un code source, vers qui puis-je me renseigner ?"

Vous pouvez contacter l'adresse électronique de contact proposée dans la politique.

Licences

"Comment choisir parmi les différentes licences proposées ?"

Voir les sections "Ouverture / Autorisation par défaut de contribuer à des projets sous licence FSF ou OSI" et "Ouverture / Autorisation par défaut de contribuer un nouveau projet avec les licences du décret".

N'hésitez pas à revenir vers nous en utilisant l'adresse de contact pour toute question ou conseil.

"J'ai besoin d'une aide juridique sur une licence Open Source, qui puis-je contacter ?"

Vous pouvez contacter l'adresse électronique de contact proposée dans la politique.

Identité électronique

"Quelle adresse électronique utiliser pour contribuer à un projet ?"

Tout est détaillé dans la page "Ouverture / Attribuer les contributions aux individus".

- et si je suis salarié d'une ESN / SSII ?

  Tout est détaillé dans la page "Ouverture / Attribuer les contributions aux individus".

- et si je suis indépendant / auto-entrepreneur ?

  Dans ce cas précis, l'identité prime et il revient au même d'utiliser une adresse électronique professionnelle ou personnelle. Choisissez ce que vous voulez.

"Dois-je utiliser mon mail pro si je contribue depuis longtemps à un projet à titre personnel ?"

Si les contributions se font dans le cadre professionnel, il vous est effectivement demandé d'utiliser votre adresse électronique professionnelle.

Divers

"Dois-je obtenir une validation avant de publier du code ?"

Bien qu'une pré-autorisation par défaut soit proposée par la DINSIC, il peut être nécessaire d'obtenir l'accord de votre supérieur hiérarchique (au même titre que vous faites valider vos formations proposées par le service formation). Pour la publication d'une nouvelle base de code et pas une contribution à un code existant, vous devrez obtenir un dépôt sur le compte de votre organisation.

"Mon administration n'a pas de compte d'organisation sur le service en ligne d'hébergement de code que je souhaite utiliser. Que faire ?"

Si votre administration dispose d'un compte sur une autre plate-forme, contactez le responsable de ce compte.

Si ce n'est pas le cas, contactez l'adresse électronique de contact proposée dans la politique.

"Je n'ose pas faire mon premier commit en public, puis-je obtenir de l'aide ?"

Si vous avez une contribution disponible sur un dépôt privé, il est possible et encouragé de demander une revue par les pairs.

Nous vous conseillons d'identifier quelqu'un au plus proche de votre structure qui a déjà contribué publiquement pour qu'il puisse vous aider.

Si toutefois vous ne parvenez pas à identifier quelqu'un, vous pouvez contacter l'adresse électronique de contact proposée dans la politique pour que nous puissions vous aider à trouver des pairs.

"Puis-je coder dans une langue autre que le français ?"

Le nom des variables et des fonctions, ainsi que les commentaires de code peuvent être rédigés dans la langue de la communauté de développeurs visée. Toutefois, la documentation utilisateur devra être disponible en français.