

Evolution du SI

V. 1.0 juillet 2019

Evolution du SI

- La fonction IT
- La stratégie IT
- L'urbanisation
- Les principes d'évolution des SI
 - cartographie du système d'information
 - Open data, Open innovation, Bring Your Own Device

Open Data : Cas des services publics

Document administratif : Il s'agit de tous les documents produits ou reçus par les administrations dans le cadre de leur mission de service public, quels que soient leur date, leur forme ou leur support.

Des données sont qualifiées de **publiques** lorsqu'elles sont produites ou collectées par l'État, une collectivité territoriale, un organe parapublic ou un délégataire dans le cadre de leurs activités de service public.

La notion de « **donnée publique** » n'existe pas dans la loi française. En revanche l'article L321-1 du CRPA (code des relations entre le public et l'administration) définit les « informations publiques » comme étant les informations contenues dans les documents administratifs

Open Data : Cas des services publics

Toute donnée faisant directement ou indirectement référence à un lieu spécifique ou une zone géographique est considérée comme une **donnée géographique** (article L127-1 du code de l'environnement). Les données géographiques sont d'un intérêt majeur dans le domaine de l'Open Data

RÉPUBLIQUE FRANÇAISE

Direction
Départementale des
Territoires
Ariège

Environnement - risques

Délégation territoriale de St Giron - Foix
agence

Direction départementale des Territoires
-DDT-

10 rue des Salenques
- Accueil de la DDT -



Administration générale

Aménagement - Urbanisme - Habitat

Connaissance et animation territoriales

Open Data : Cas des services publics

L'article 4 du RGPD définit la notion de **donnée à caractère personnel** par : « toute information se rapportant à une personne physique identifiée ou identifiable ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; ».

Open Data : Cas des services publics

Cas des **données personnelles sensibles**.

Les données de type médicale, génétique, politique, syndicale, philosophique, ayant trait à la sexualité, ethnique, raciale, infractions ou condamnations pénales, numéro de sécurité sociale ne doivent pas être collectées par principe.

Si on doit le faire, on doit pouvoir le justifier et prendre toutes les précautions légales nécessaires.

Open Data : Cas des services publics

Le service public de la donnée créé par la loi pour une République numérique vise à mettre à disposition, en vue de faciliter leur réutilisation, les jeux de données de référence qui présentent le plus fort impact économique et social.

Au 1er janvier 2018, 9 jeux de données de référence sont identifiés :

- Base adresse nationale (BAN)
- Base Sirene des entreprises et de leurs établissements (SIREN, SIRET)
- Code officiel géographique (COG)
- Plan cadastral informatisé (PCI)
- Registre parcellaire graphique (RPG) : contours des îlots cultureux et leurs groupe de culture majoritaire
- Référentiel de l'organisation administrative de l'Etat
- Référentiel à grande échelle (RGE)
- Répertoire national des associations (RNA)

Open Data : Cas des services publics

L'Open Data repose sur trois principes fondamentaux :

- la connaissance des données existantes ;

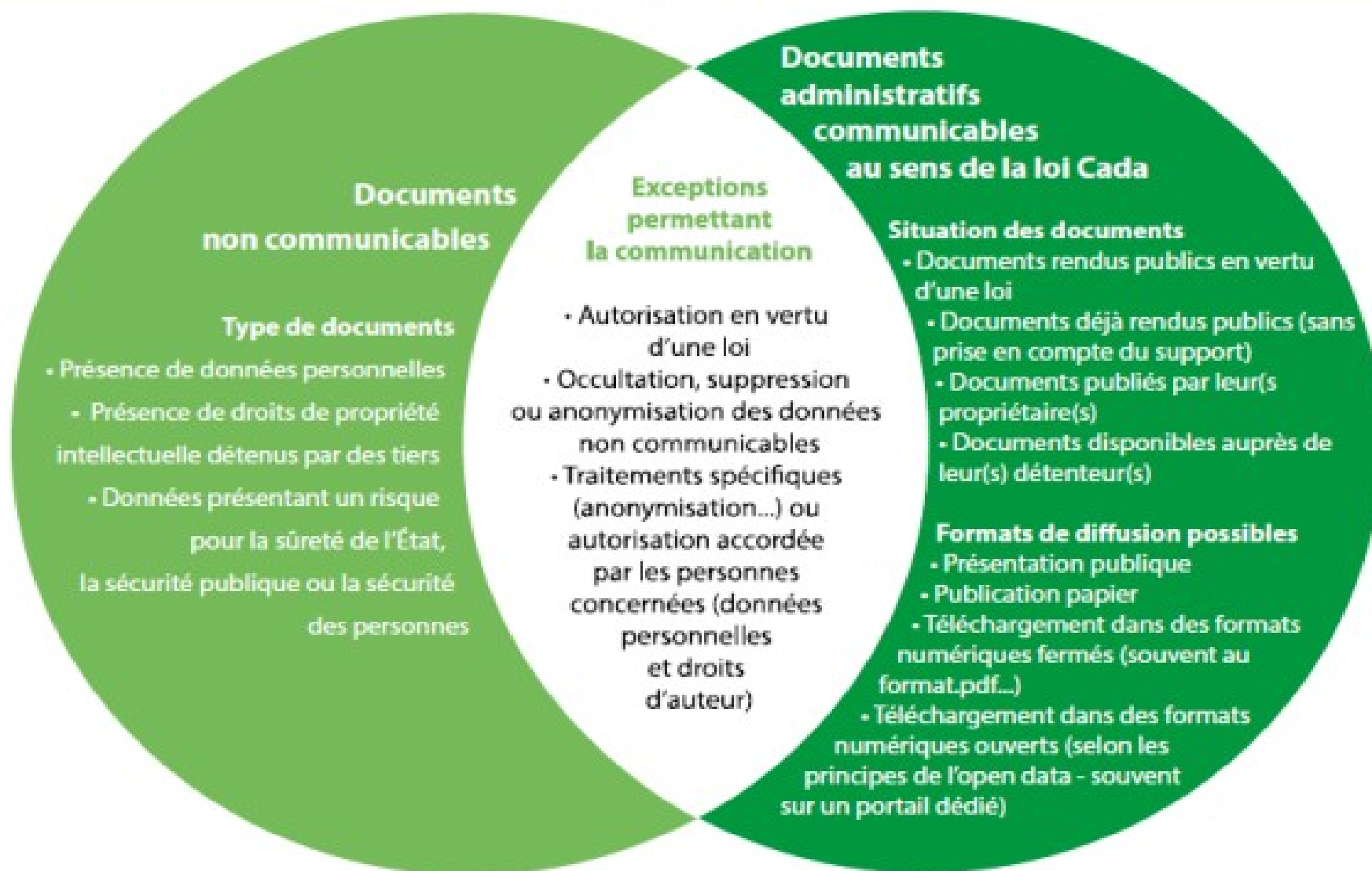
- le libre accès aux données ;

- le droit de réutilisation des données quel qu'en soit l'objectif.

La loi impose aux administrations (État, collectivités, établissements publics ...) d'ouvrir largement l'accès à leurs données, de les faire connaître et d'en autoriser la réutilisation.

Open Data : Cas des services publics

DOCUMENTS ADMINISTRATIFS*



Open Data : Cas des services publics

La loi française indique que les informations publiques peuvent être réutilisées par toute personne qui le souhaite. Elle n'impose pas de limitation quant à l'objectif de réutilisation poursuivi ; il peut donc être à but commercial.

Le ré-utilisateur a pour seuls devoirs de :

- ne pas altérer les informations
- ne pas dénaturer leur sens
- citer la source des informations ainsi que leur dernière date de mise à jour

Direction départementale des Territoires
-DDT-

10 rue des Salenques
- Accueil de la DDT -



Direction

Administration générale

Aménagement - Urbanisme - Habitat

Connaissance et animation territoriales

Open Data : Cas des services publics

Au titre des articles L323-2 et suivants du CRPA, seules deux licences peuvent être utilisées par les administrations pour accompagner la réutilisation gratuite de leurs données :

- la licence ouverte de réutilisation d'informations publiques (parfois appelée **licence Etalab**)
- la **licence ODbL** (Open Database License)

Open Data : Quizz 3

RÉPUBLIQUE FRANÇAISE
Direction
Départementale des
Territoires
Ariège

← 1 rue Fenouillet

? QUIZ
TIME

10 rue des Salenques →

Direction

Administration générale

Aménagement - Urbanisme - Habitat

Connaissance et animation territoriales

Direction départementale des Territoires
-DDT-

10 rue des Salenques
- Accueil de la DDT -



Open Data : Cycle de vie

Au sein d'une administration

- Décision stratégique - Conception / Validation de la base
- acquisition / validation technique (ex. saisie d'un formulaire, comptage automatique, ...)
- vie de la donnée (qualité) / validation métier

Réutilisation open data / export

Archivage : destruction



10 rue des Salenques

Direction

Administration générale

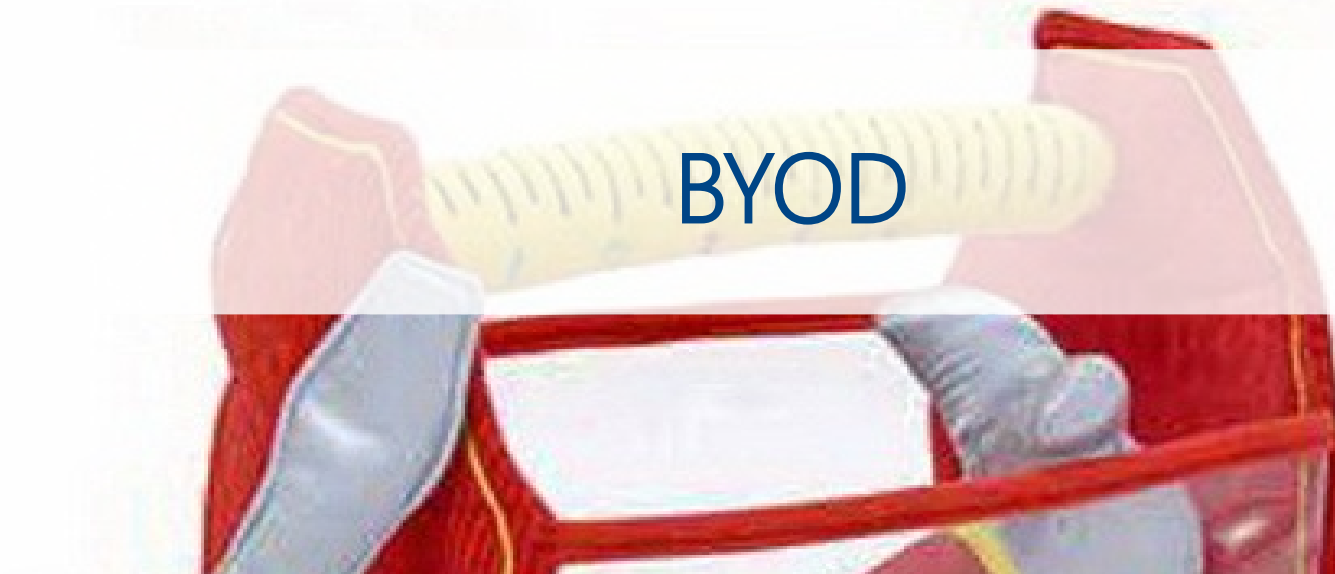
Aménagement - Urbanisme - Habitat

Connaissance et animation territoriales

Direction départementale des Territoires
-DDT-

10 rue des Salenques
- Accueil de la DDT -





BYOD

« BYOD » est l'abréviation de l'expression anglaise « Bring Your Own Device » (en français : « Apportez Votre Équipement personnel de Communication »), qui désigne l'usage d'équipements informatiques personnels dans un contexte professionnel.



BYOD

que :

- se connecter de façon sécurisée au SI
- collecter et de traiter des données personnelles
- assurer la sécurité de l'environnement professionnel

-

BYOD



Les risques contre lesquels il est indispensable de se prémunir :

- l'atteinte ponctuelle à la disponibilité,
- l'intégrité et la confidentialité des données,
- à la compromission générale du système d'information de l'entreprise (intrusion, virus, chevaux de Troie, etc.).

BYOD



Comment réduire ces risques ?

- identifier les risques, en tenant compte des spécificités du contexte (quels équipements, quelles applications, quelles données ?), et les estimer en termes de gravité et de vraisemblance.
- déterminer les mesures à mettre en œuvre et les formaliser dans une politique de sécurité.

BYOD : réduire les risques

- **cloisonner** les parties de l'outil personnel ayant vocation à être utilisées dans un cadre professionnel (création d'une « bulle de sécurité ») ;
- **contrôler l'accès distant** par un dispositif d'authentification robuste de l'utilisateur (si possible à l'aide d'un certificat électronique, d'une carte à puce, etc.) ;
- mettre en place des mesures de **chiffrement des flux** d'informations (VPN, HTTPS, etc.) ;

BYOD : réduire les risques

- prévoir une **procédure en cas de panne/perte** du terminal personnel (information de l'administrateur réseau, mise à disposition d'un équipement alternatif professionnel, effacement à distance des données professionnelles stockées sur le terminal personnel) ;
- exiger le **respect de mesures de sécurité élémentaires** telles que le verrouillage du terminal avec un mot de passe conforme aux bonnes pratiques et l'utilisation d'un antivirus à jour ;

BYOD : réduire les risques

- **sensibiliser** les utilisateurs aux risques, **formaliser les responsabilités** de chacun et préciser les précautions à prendre dans une charte ayant valeur contraignante ;
- subordonner l'utilisation des équipements personnels à une **autorisation préalable** de l'administrateur réseau et/ou de l'employeur.

BYOD : vie privée

- Il n'est pas possible de prévoir des mesures de sécurité ayant pour objet ou effet d'entraver l'utilisation d'un BYOD dans un cadre privé.
- l'employeur ne peut accéder à des éléments relevant de la vie privée stockés dans l'espace personnel de l'équipement (liste des sites internet consultés, photos, films, agenda, annuaire).
- Un effacement à distance ne peut se faire que sur les données d'entreprises.

BYOD : loi

Les textes de référence

- Code du travail - Article L. 1121-1 (protection des droits fondamentaux des salariés)
- Code du travail - Article L. 1222-4 (information des salariés)
- Article L. 2312-38 (information et consultation du comité social et économique)
- Code civil - Article 9 (protection de l'intimité de la vie privée)
- loi « Informatique et libertés » - Article 2
- loi « Informatique et libertés » - Article 34 (sécurité des données)

BYOD : exercice

Vous diriger une société d'aide à la personne. Certains de vos collaborateurs ont émis le souhait de pouvoir utiliser leur propre matériel dans le cadre de leur travail :

- Check à l'arrivée et au départ de leurs séance de travail chez un client (service propulsé par l'entreprise)
- Saisie du rapport d'intervention (texte)
Transmission du rapport d'intervention (mail sur adresse d'entreprise)

Gisèle, salariée depuis 5 ans, mariée et mère de deux enfants en collège sera la première à tester le BYOD. Ses visites l'amène à travailler avec des personnes âgées fragilisées. Elle utilisera son propre ordinateur portable. Elle prend régulièrement les transports en commun.

BYOD : exercice

- D'après vous, comment doit-elle organiser techniquement son travail sur sa machine ?
- Quels composants de sécurité doit-elle installer ?
- Quels scénarios d'incidents (réalistes et probables) peut-on imaginer ?
- Détailler l'ensemble des mesures préconisées pour gérer au mieux ces risques et scénarios.

Bibliographie

L'ouverture des données publiques : nouvelles obligations et nouveaux acteurs - Inno3 - juin 2017 - <http://inno3.fr/ressources/livre-blanc-louverture-des-donnees-publiques-nouvelles-obligations-et-nouveaux-acteurs>

Vade-mecum sur l'ouverture et le partage des données publiques

Vade-mecum sur l'ouverture et le partage des données publiques - Etalab - Septembre 2013 - <http://www.modernisation.gouv.fr/laction-publique-se-transforme/en-ouvrant-les-donnees-publiques/lopen-data-son-vade-mecum>

Livre blanc sur les données ouvertes

Livre blanc sur les données ouvertes - ISH - 2015 - <https://halshs.archives-ouvertes.fr/halshs-01162692>

Fiches pédagogiques "Ouverture des données publiques"

Fiches pédagogiques "Ouverture des données publiques" - OpenDataFrance - <https://docs.google.com/document/d/12OFaur5pbu5ltQtpUEi16w2yu0359sm6rbjG7hH8Jic/edit>
Les 8 principes de la donnée ouverte

The 8 Principles of Open Government Data - Joshua Tauberer - <https://opengovdata.org/>

<https://eformation.cerema.fr>, « l'open data et vous », mars 2018

<https://openclassrooms.com/fr/courses/2100086-decouvrez-le-monde-des-systemes-dinformation/5598421-maitrisez-l-impact-du-data-management-sur-le-si>