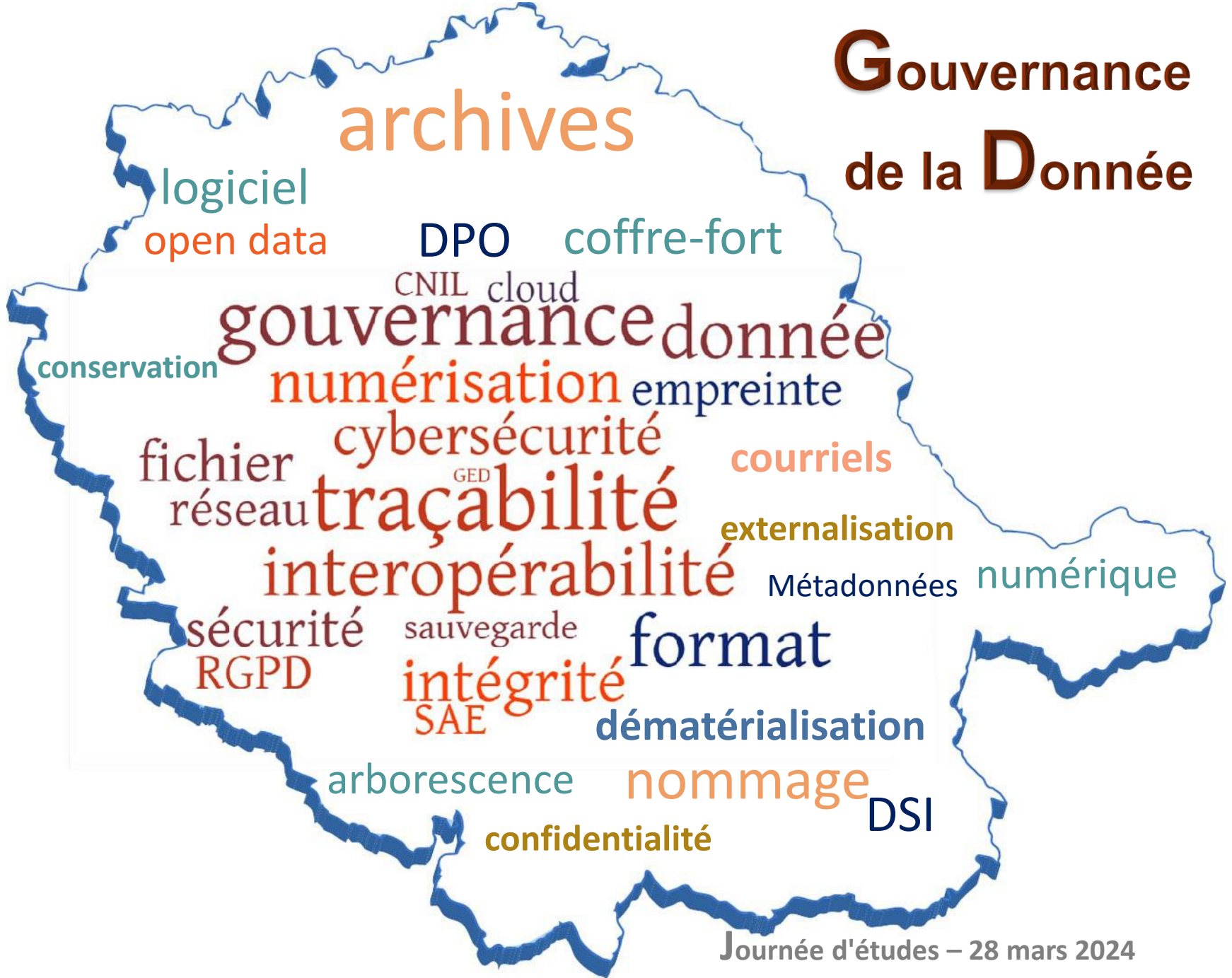


Gouvernance de la Donnée



Gouvernance de la donnée

Programme

10h / 10h15	Introduction : contexte et objectifs
10h15 / 11h30	Restitution des travaux du Comité d'experts de la donnée du Tarn
11h30 / 12h00	Actions à mener et perspectives
12h00 / 12h30	Échanges – discussions

Gouvernance de la donnée

Contexte

Définir les procédures et les responsabilités pour assurer la qualité et la sécurité des données au sein de la collectivité

Il s'agit de :

- **Archivage électronique des communes : axe de travail motivé par le Contrôle Scientifique et Technique (CST)**
- **Sujet majeur et structurant**
- **Attente** des collectivités territoriales
- **Demande** d'accompagnement
- **Enjeux** juridiques, financiers et économiques

Gouvernance de la donnée

Objectifs

Démarche volontaire d'accompagnement

- **Journée d'études : pourquoi ?**

Favoriser les rencontres autour de la question de la donnée

Créer une dynamique

- **Trois actions**

1. Sensibiliser les élus, les DSI, les DPO, les services producteurs

2. Connaître / faire connaître le traitement de la donnée

3. Apporter de la méthode, des outils, procurer conseil et assistance



Comité d'experts de la donnée du Tarn

Groupe interdisciplinaire : archivistes, DSI, DPO

1. Archiviste

Obligation d'organiser la gestion des données publiques sur le territoire

2. DPO

Gestion et expertise liée à la protection des données personnelles (RGPD)

3. DSI

Acteur majeur, incontournable de la transformation numérique

4. Association des Maires du Tarn

Délégué à la protection des données mutualisé et Assistance numérique

5. Centre de Gestion du Tarn

Mission d'assistance à l'archivage auprès des collectivités



Comité d'experts de la donnée du Tarn

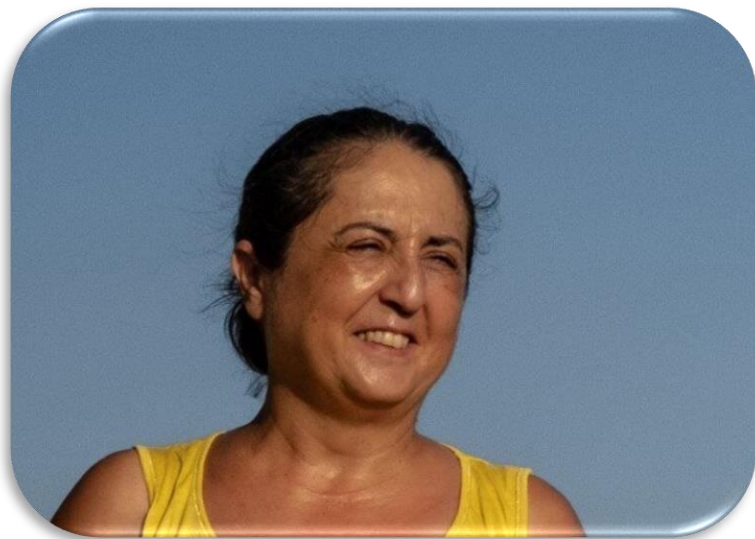
4 axes de travail

1. Rédaction de fiches à destination des collectivités
2. Proposition d'une arborescence bureautique
3. Priorisation des données communales et intercommunales
4. Établissement d'un questionnaire et d'une grille d'enquête



Comité d'experts de la donnée du Tarn

Rédaction de fiches



*Isabelle Mas
archiviste*

Communauté d'agglomération Gaillac-Graulhet



*Brigitte Bourgade
archiviste*

Ville de Carmaux



Fiche 10 Externaliser la conservation de ses données numériques

L'externalisation de la conservation des données est un aspect juridique et technique complexe : que peut-on externaliser ? Comment ? Où ? Pendant quelle durée ? Avec quelle maîtrise de ce qui est externalisé ?

Le champ de l'externalisation

L'externalisation de la conservation des données numériques doit être abordée sous son aspect le plus large, celui des archives. En ce sens, le code du patrimoine, dans son article L212-1 est précis et structurant : « Les archives sont l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé, dans l'exercice de leur activité. »

Cette définition ne préjuge donc ni du producteur, ni de la forme (état ou états successifs), ni du support, ni de la date. Pour ce qui relève de nos collectivités territoriales, il s'agit d'archives publiques (Art. L212-4 du CP). Ces archives pourront être d'utilisation courante (Art. L212-2 du CP) ou destinées à être conservées (Art. L212-4 ou CP).

Qu'en est-il de l'externalisation de la conservation de données numériques en regard d'archives définitives ?

Les articles L 212-6 à L 212-14 du code du patrimoine encadrent le sort des archives publiques, qui sont administrées par les collectivités sous le contrôle scientifique et technique de l'État. Il n'est pas possible d'externaliser la conservation d'archives définitives. Elles doivent être conservées dans un service public d'archives, ce qui veut également signifier sans dématérialisation.

Pour cette catégorie d'archives dématérialisées, il convient de distinguer « gestion des archives » et « hébergement des archives » : l'hébergement par un prestataire tiers, dans un datacenter externe, peut aussi bien être la responsabilité et les opérations liées aux documents et données restent entièrement du ressort du service public d'archives. Il est donc possible pour une collectivité de recourir à une prestation de type PaaS (plateforme as a service) pour l'hébergement de son système d'archivage électronique (SAE) pourvu que son service d'archives en garde la maîtrise. Inversement, confier la responsabilité de la gestion et de l'hébergement à un tiers n'est pas un mécanisme de mutualisation entre collectivités et leur service public d'archives, mutualité qui suppose un accord de principe.

Et pour les données numériques courantes ?

De manière générale, il est possible de confier la gestion et l'hébergement de données numériques courantes et intermédiaires à un prestataire tiers, après accord par le service interministériel France. Une déclaration préalable, et en cas de doute adressée à l'administration des archives, est recommandée.



Externaliser la conservation de ses données numériques

On peut faire beaucoup, mais tout n'est pas possible...

Le champ de l'externalisation

Les données numériques d'une collectivité sont des données publiques définies par le code du patrimoine (Art. L212-2 et 4).

Le code du patrimoine encadre l'externalisation des archives

Il n'est pas possible d'externaliser la conservation de données numériques qui sont des archives définitives d'un service public d'archives.

L'hébergement des archives définitives par un prestataire tiers, dans un datacenter externe, est néanmoins possible si la responsabilité et les opérations liées aux documents et données restent entièrement du ressort du service public d'archives.

Il est possible d'externaliser les archives publiques courantes, mais le prestataire doit être agréé par le service interministériel des archives de France (désormais France Archives) pour assurer la conservation de ces données.

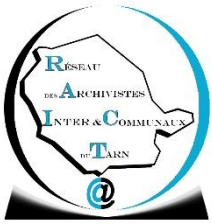
Cas particulier : un service public d'archives, ainsi que ses prestataires tiers, peut être autorisé à mutualiser ses données numériques avec d'autres collectivités territoriales et services publics d'archives, sous réserve de la protection des données et de la sécurité des données.



Fiches référentiels

Rédaction de fiches

- Facilité d'utilisation
- Éventail thématique
- Praticité
- Gain de temps



Fiches référentiels

Rédaction de fiches

2 types

□ Un référentiel « dossier »

- fiches détaillées avec des références juridiques
- Format A4 / recto verso

Fiche 4 **Traiter le wrac numérique : méthode et outils**

Définition

Les documents en wrac sont des documents nativement numériques (documents bureautiques, vidéos et photos, mails enregistrés, etc.) et/ou les documents scannés stockés sur des outils de partage de l'information ou sur des volumes partagés en réseau. Un « wrac » est défini dans l'Abbrégé archivistique comme « un fonds qui se présente sans aucun classement apparent et dont la provenance peut ne pas être identifiée. »

Dans le contexte numérique, un wrac peut donc être caractérisé par :

- une absence de contextualisation (producteur et/ou missions non connus)
- une hétérogénéité du contenu
- un mélange des éléments (sans arborescence/originaux, copies, versions intermédiaires, finales difficiles à retrouver)
- une absence d'identification des contenus (nommage non significatif/peu ou pas de métadonnées de contexte, techniques et/ou descriptives)
- un stockage aléatoire (serveur, clé USB, disque dur externe)
- une notion de conditionnement qui n'est plus matérielle avec parfois l'existence d'un fonds papier en parallèle (identique ou complémentaire)

De là, découlent des problèmes :

- ▶ d'identification : où se trouve le document engageant
- ▶ de volume : plus de place et/ou amoncellement de fichiers sur un serveur
- ▶ de lecture : lisibilité des formats qui ne sont plus maintenus
- ▶ de contextualisation
- ▶ de gestion d'une production mixte (papier/numérique)

Méthodologie

Sensibilisation des services

Formaliser en amont des éléments méthodologiques, en collaboration avec le service informatique, à destination des services afin de lever le sentiment de confusion des agents pour instaurer de bonnes pratiques et éviter la constitution de wrac numérique.

- guides, fiches-conseils, chartes, etc.
- formations
- ateliers pratiques (par exemple, opérations dites de « ménage informatique »)
- mise à disposition d'un kit d'outils pour le tri de documents bureautiques

Étape de traitement d'un wrac numérique

Deux questions principales sont à se poser :

- Est-il utile de traiter ce wrac ?
- Quel niveau de traitement vais-je lui appliquer ?

Fiche 4 Identifier les phases pour la prise en charge d'un wrac numérique :

- Phase 1 – Évaluation
- Phase 2 – Actions
- Phase 3 – Transfert

Pour en savoir plus : BECHAM LORRIS, PUNTES HÉLÈNE, LORRIS VASSAL, Édouard, Les archives numériques, Paris, AAF, « Poches guides des archives », 2014, 86 p.

Les outils de traitement

Cette liste n'est pas exhaustive et dans tous les cas, rapprochez vous de votre service informatique pour trouver un outil adapté ou bénéficier de son aide. À noter que dans un souci de traçabilité, il est souhaitable de conserver les rapports produits lors de l'utilisation des outils logiciels.

Transfert de fichiers bureautiques

- Robocopy**
Éditeur Microsoft Windows.
Licence Microsoft Corporation ID
- Data Accessioner**
Éditeur David M. Rubenstein
Rare Book and Manuscript Library of the University Duke.
Licence libre

Identification des formats de fichiers

- Droid**
Éditeur Archives nationales du Royaume-Uni.
Licence New BSD Licence

Explorer et auditer un fonds

- Lud**
Éditeur Chagrin
<http://lud.one.fr-FR>
- Windirstat**
Éditeur Olivier Schneider
<https://windirstat.net>
- Archifiltre**
Éditeur Mission des Archives de France auprès des ministères sociaux
<https://archifiltre.github.io>

Reperage et élimination des doublons

- Alldup**
Éditeur Michael Thummerer
Software Design
http://www.alldup.de/en_index.php

Reommage des fichiers

- Ant Renamer**
Éditeur Antoine Potten
<http://www.antp.be/software/renamer/sources/fr>
- XnView**
Éditeur Pierre-Emmanuel Gougelet
<https://www.xnview.com/fr>

Description d'un mouvement bureautique et empilement

- Octave**
Éditeur Archives de France
<https://francearchives.fr/fr/article/88482499>
- Resip**
Éditeur Programme VITAM
<https://www.programmevitam.fr/pages/ressources/resip/contact>
@programmevitam.fr



Fiches référentiels

Rédaction de fiches

□ Un référentiel « synthétique »

- fiches ludiques, simple à utiliser
- 1/3 format paysage sur feuille A4

Fiche
9

LA CYBERSÉCURITÉ :

Des risques auxquels nous sommes tous confrontés

COMMENT SE PROTÉGER ?

En cas de cyberattaque, la responsabilité de la collectivité peut être engagée sur le plan administratif, civil et pénal.

Les principaux types de cyberattaques :

Rançongiciel, hameçonnage, déni de service, cybersabotage peuvent avoir de lourdes conséquences : sites bloqués, vol de données personnelles, missions de service public interrompues.

◆ Le facteur humain représente l'essentiel des facteurs de risque, d'où l'importance d'adopter des bonnes pratiques.

Un accompagnement et une sensibilisation

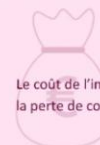
L'ANSSI (Agence nationale de la Sécurité des Systèmes d'Information) : <https://www.ssi.gouv.fr> et la plateforme <https://www.cybermalveillance.gouv.fr> vous aident à vous prémunir des attaques et vous accompagnent lorsque le risque est devenu réalité.

Les bonnes pratiques

- ◆ Les bonnes pratiques doivent concerner TOUS les appareils connectés
 - des mots de passe sécurisés
 - des sauvegardes et mises à jour régulières
 - des usages pro-perso encadrés

◆ Les documents numériques et papier doivent être traités de manière égale et faire l'objet d'un bordereau d'élimination soumis pour accord aux Archives départementales.

Fiche
9



Le coût de l'insécurité peut être considérable, ainsi que la perte de confiance dans la collectivité.

QUESTIONS

Connaissez-vous les conséquences que peut avoir une cyberattaque sur votre collectivité ?

En cas d'incident de cybersécurité, devez-vous le notifier aux autorités ?

La cybersécurité concerne-t-elle uniquement votre Direction des Services Informatiques (DSI) ?

Avez-vous mis en place un plan de gestion de crise ?



Besoin d'aide ?

Contactez les Archives départementales !
archives.tarn@tarn.fr





Liste des fiches

Rédaction de fiches

- Fiche 1 La donnée numérique : normes et enjeux
- Fiche 2 Les essentiels : vocabulaire
- Fiche 3 Gérer et conserver **ses** fichiers numériques (arborescence)
- Fiche 4 Traiter le vrac bureautique
- Fiche 5 Gérer vos courriers électroniques
- Fiche 6 La protection des données personnelles (RGPD)
- Fiche 7 Numérisation et dématérialisation
- Fiche 8 Le système d'archivage électronique
- Fiche 9 La cyber sécurité
- Fiche 10 Externalisation de la conservation des données



Présentation d'une fiche détaillée la cybersécurité

Fiche
9

La cybersécurité

La transformation numérique vécue actuellement par les collectivités territoriales, quelle que soit leur taille, est source d'opportunités et de risques (sites bloqués, vol de données personnelles, missions de service public interrompues...).



Comprendre les risques et réagir

Rançongiciel ou ransomware

virus informatique qui rend indisponible un système ou des données tant qu'une rançon n'a pas été payée



Hameçonnage ou phishing :

cyberattaque consistant à appâter une personne pour lui faire exécuter une action nuisible, comme l'ouverture d'une pièce jointe corrompue ou d'un lien pointant vers un site malveillant.



Déni de service

attaque contre un serveur ou un site internet ; consistant à le saturer de requêtes afin de le rendre indisponible

D.O.S



Cybersabotage

cyberattaque visant à rendre indisponible ou faire dysfonctionner un système, un service, une infrastructure



Les collectivités territoriales ne sont pas seules face aux risques

L'ANSSI (Agence nationale de la Sécurité des Systèmes d'Information)
<https://www.ssi.gov.fr>

et la plate-forme <https://www.cybermalveillance.gouv.fr>

aident à se prémunir des attaques et accompagnent lorsque le risque est devenu réalité



Quelques recommandations

Sensibiliser les acteurs aux enjeux de la cybercriminalité. Les actions de **formation**, d'accompagnement, sont essentielles pour mener une vraie politique de sécurité numérique :

- rédaction d'une **charte** informatique à valeur contraignante,
- désignation d'un **référént** cybersécurité...

Fiche
9

Pour répondre à ces enjeux, [Cybermalveillance.gouv.fr](https://www.cybermalveillance.gouv.fr) a conçu, en partenariat avec l'Association des maires de France et des présidents d'intercommunalité (AMF), une **méthodologie** « clé en main » pour sensibiliser l'ensemble des agents aux risques cyber.



<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybersecurite-methode-cle-sensibiliser-agents-collectivites>

Les bonnes pratiques

L'hygiène de base concerne TOUS les appareils connectés (ordinateur portable, smartphone...)

- Les mots de passe : un outil permet de générer un mot de passe solide : <https://www.cnil.fr/fr/generer-un-mot-de-passe-solide>
- La mise en place d'une **procédure automatique de verrouillage de session** est un gage de sécurité supplémentaire
- Les **usages pro-perso** : messageries professionnelle et personnelle doivent être distinctes. Il est également déconseillé d'utiliser le système de stockage professionnel à des fins personnelles ou vice versa
- Porter une attention particulière aux sauvegardes et mises à jour



Les documents numériques et papier doivent être traités de manière égale et faire l'objet d'un bordereau d'élimination soumis pour accord aux archives départementales

Le coût de l'insécurité pouvant être considérable, il est important que communes et intercommunalités mettent en place une réflexion commune sur le renforcement de la sécurité numérique.

Il est fortement conseillé de porter plainte pour atteinte à un traitement automatisé de données en cas d'acte de cybermalveillance et de faire une déclaration à la CNIL lorsque l'incident implique des données à caractère personnel.





Présentation d'une fiche synthétique la cybersécurité

Fiche
9

LA CYBERSÉCURITÉ :

Des risques auxquels
nous sommes tous confrontés

COMMENT SE PROTÉGER ?

En cas de cyberattaque,
la responsabilité de la collectivité peut être engagée
sur le plan administratif, civil et pénal.

Les principaux types de cyberattaques :

Rançongiciel, hameçonnage, déni de service, cybersabotage
peuvent avoir de lourdes conséquences : sites bloqués,
vol de données personnelles, missions de service public
interrompues.

- ◆ Le facteur humain représente l'essentiel des facteurs
de risque, d'où l'importance d'adopter des bonnes
pratiques.

Un accompagnement et une sensibilisation

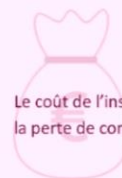
L'ANSSI (Agence nationale de la Sécurité des Systèmes
d'Information) : <https://www.ssi.gouv.fr>
et la plateforme <https://www.cybermalveillance.gouv.fr>
vous aident à vous prémunir des attaques et vous accom-
pagnent lorsque le risque est devenu réalité.

Les bonnes pratiques

- ◆ Les bonnes pratiques doivent concerner TOUS les
appareils connectés
 - des mots de passe sécurisés
 - des sauvegardes et mises à jour régulières
 - des usages pro-perso encadrés
- ◆ Les documents numériques et papier doivent être
traités de manière égale et faire l'objet d'un borde-
reau d'élimination soumis pour accord aux Archives
départementales.



Fiche
9



Le coût de l'insécurité peut être considérable, ainsi que
la perte de confiance dans la collectivité.

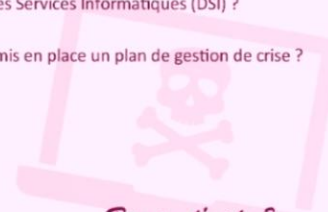
QUESTIONS

Connaissez-vous les conséquences que peut avoir une
cyberattaque sur votre collectivité ?

En cas d'incident de cybersécurité, devez-vous le notifier
aux autorités ?

La cybersécurité concerne-t-elle uniquement votre
Direction des Services Informatiques (DSI) ?

Avez-vous mis en place un plan de gestion de crise ?



Besoin d'aide ?

Contactez les Archives départementales !
archives.tarn@tarn.fr





Où se procurer les fiches

Rédaction de fiches

Gouvernance de la donnée numérique

Fiches référentiels détaillées et synthétiques

conçues par le Comité d'experts de la donnée du Tarn

Groupe de travail interdisciplinaire (archivistes, DSI / DPO)



2023

- Fiche 1. *La donnée numérique : les enjeux et les normes*
- Fiche 2. *Lexique : les notions essentielles*
- Fiche 3. *Gérer et conserver ses fichiers numériques*
- Fiche 4. *Traiter le vrac numérique : méthode et outils*
- Fiche 5. *Gérer vos courriers électroniques*
- Fiche 6. *Le RGPD : Règlement général sur la protection des données*
- Fiche 7. *Numérisation et dématérialisation*
- Fiche 8. *Le système d'archivage électronique (SAE)*
- Fiche 9. *La cybersécurité*
- Fiche 10. *Externaliser la conservation de ses données numériques*



2 supports de diffusion

- ❑ Porte-fiches (distribué à la sortie)
- ❑ Version numérique à télécharger sur les sites de :
 - l'Association des Maires du Tarn
 - du Centre de Gestion du Tarn
 - ou des Archives départementales

[référentiels](#)

Rédaction de fiches



Fiche 10 Externaliser la conservation de ses données numériques

L'externalisation de la conservation des données est un aspect juridique et technique complexe : que peut-on externaliser ? Comment ? Où ? Pendant quelle durée ? Avec quelle maîtrise de ce qui est externalisé ?

Le champ de l'externalisation

L'externalisation de la conservation des données numériques doit être abordée sous son aspect le plus large, celui des archives. En ce sens, le code du patrimoine, dans son article L212-1 est précis et structurant : « Les archives sont l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé, dans l'exercice de leur activité. »

Cette définition ne préjuge donc ni du producteur, ni de la forme (état ou états successifs), ni du support, ni de la date. Pour ce qui relève de nos collectivités territoriales, il s'agit d'archives publiques (Art. L212-4 du CP). Ces archives pourront être d'utilisation courante (Art. L212-2 du CP) ou destinées à être conservées (Art. L212-4 ou CP).

Qu'en est-il de l'externalisation de la conservation de données numériques ayant statut d'archives définitives

Les articles L 212-6 à L 212-14 du code du patrimoine encadrent le sort des archives publiques, qui sont administrées par les collectivités sous le contrôle scientifique et technique de l'État. Il n'est pas possible d'externaliser la conservation d'archives définitives. Elles doivent être conservées dans un service public d'archives, ce qui veut également dire qu'elles sont dématérialisées.

Pour cette catégorie d'archives dématérialisées, il convient de distinguer « gestion des archives » et « hébergement des archives » : l'hébergement par un prestataire tiers, dans un datacenter externe, est possible si la responsabilité et les opérations liées aux documents et données restent entièrement du ressort du service public d'archives. Il est donc possible pour une collectivité de recourir à une prestation de type PaaS (plateforme as a service) pour l'hébergement de son système d'archivage électronique (SAE) ouvert ou son service d'archives en garde la maîtrise. Inversement, confier la responsabilité de la gestion et de l'hébergement à un tiers n'est pas possible sans un mécanisme de mutualisation entre collectivités et leur service public d'archives, mutualité qui s'appuie sur un accord de principe.

Et pour les données numériques ayant statut d'archives courantes

De manière générale, il est possible de confier la gestion et l'hébergement de données numériques courantes et intermédiaires à un prestataire tiers, après accord par le service interministériel France. Une déclaration préalable, et en cas de données sensibles, une autorisation préalable, doivent être adressés à l'administration des données.

Comprendre l'externalisation

La transmission de données numériques est soumise à des règles strictes. Le champ de l'externalisation est défini par le code du patrimoine.

Ransom : une information qui rend inopérant un système de sécurité, quel qu'il soit, sans que l'utilisateur en ait conscience.

Le champ de l'externalisation

L'externalisation de la conservation des données numériques doit être abordée sous son aspect le plus large, celui des archives. En ce sens, le code du patrimoine, dans son article L212-1 est précis et structurant : « Les archives sont l'ensemble des documents, y compris les données, quels que soient leur date, leur lieu de conservation, leur forme et leur support, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé, dans l'exercice de leur activité. »

Cette définition ne préjuge donc ni du producteur, ni de la forme (état ou états successifs), ni du support, ni de la date. Pour ce qui relève de nos collectivités territoriales, il s'agit d'archives publiques (Art. L212-4 du CP). Ces archives pourront être d'utilisation courante (Art. L212-2 du CP) ou destinées à être conservées (Art. L212-4 ou CP).

Qu'en est-il de l'externalisation de la conservation de données numériques ayant statut d'archives définitives

Les articles L 212-6 à L 212-14 du code du patrimoine encadrent le sort des archives publiques, qui sont administrées par les collectivités sous le contrôle scientifique et technique de l'État. Il n'est pas possible d'externaliser la conservation d'archives définitives. Elles doivent être conservées dans un service public d'archives, ce qui veut également dire qu'elles sont dématérialisées.

Pour cette catégorie d'archives dématérialisées, il convient de distinguer « gestion des archives » et « hébergement des archives » : l'hébergement par un prestataire tiers, dans un datacenter externe, est possible si la responsabilité et les opérations liées aux documents et données restent entièrement du ressort du service public d'archives. Il est donc possible pour une collectivité de recourir à une prestation de type PaaS (plateforme as a service) pour l'hébergement de son système d'archivage électronique (SAE) ouvert ou son service d'archives en garde la maîtrise. Inversement, confier la responsabilité de la gestion et de l'hébergement à un tiers n'est pas possible sans un mécanisme de mutualisation entre collectivités et leur service public d'archives, mutualité qui s'appuie sur un accord de principe.

Et pour les données numériques ayant statut d'archives courantes

De manière générale, il est possible de confier la gestion et l'hébergement de données numériques courantes et intermédiaires à un prestataire tiers, après accord par le service interministériel France. Une déclaration préalable, et en cas de données sensibles, une autorisation préalable, doivent être adressés à l'administration des données.

Comprendre l'externalisation

La transmission de données numériques est soumise à des règles strictes. Le champ de l'externalisation est défini par le code du patrimoine.

Ransom : une information qui rend inopérant un système de sécurité, quel qu'il soit, sans que l'utilisateur en ait conscience.





Comité d'experts de la donnée du Tarn

Construire une arborescence



Françoise CAYRE
archiviste

Archives départementales du Tarn

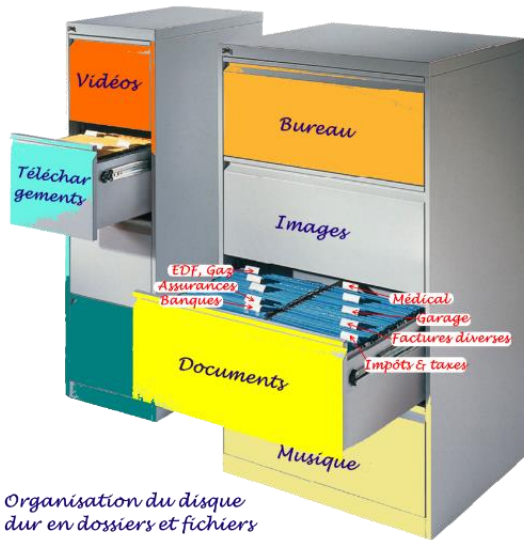


Oumar KANDÉ
archiviste itinérant

Centre de gestion du Tarn



Constitution d'une arborescence bureautique



Organisation du disque dur en dossiers et fichiers

De quoi parle-t-on ?

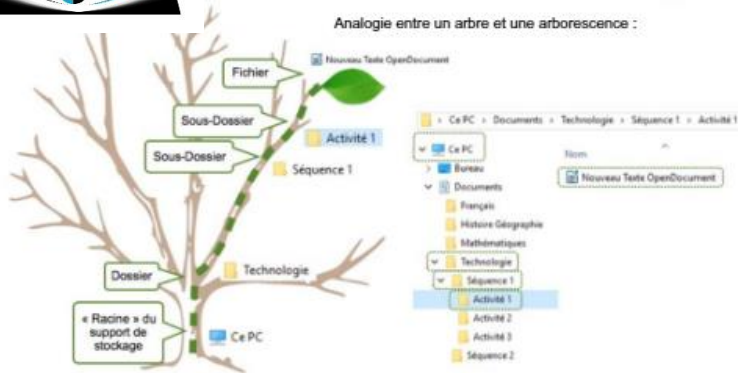
- **Plan de classement des documents bureautiques** produits et reçus au quotidien par les services
 - Permet de **ranger ses dossiers** de manière structurée dans un espace commun
- **Structure hiérarchisée par niveau** des répertoires et des sous-répertoires permettant d'anticiper de manière cohérente les opérations d'archivage



Quelques principes et conseils

Construire une arborescence

Analogie entre un arbre et une arborescence :



- Repérer **les missions et activités de la collectivité et le rôle des agents**
- Élaborer un plan de classement qui va du **général au particulier**
- Respecter **les limitations techniques** (256 caractères pour une arborescence complète)
- **Numéroter** chaque niveau
- Établir une **charte de nommage des fichiers**
- Se conformer au **RGPD** (Règlement général sur la Protection des données)



Proposition d'une arborescence bureautique

Construire une arborescence

- **Établie selon l'organisation fonctionnelle de la collectivité**
(pôles, directions, services)

- **Conforme aux calendriers de conservation et d'éliminations des archives**
(circulaires du SIAF « Service Interministériel des Archives de France » 2009 et 2014)
 - 📁 1^{er} niveau structurant pour la collectivité
entre [] une variante abrégée pour limiter la longueur

 - 📁 2^{ème} niveau structurant pour ses services

 - 📁 3^{ème} niveau structurant, par thème ou type de dossier traité



NIVEAU 1

Construire une arborescence

01_Administration_generale	[01_ADGEN]
02_Ressources_humaines	[02_RH]
03_Finances	[03_FIN]
04_Commande_publicque	[04_MP]
05_Patrimoine_immobilier_mobilier	[05_PIM]
06_Services_support	[05_SSUP]
07_Politique_de_la_ville	[06_POLVIL]
08_Population	[07_POP]
09_Amenagement_urbain	[09_AMUR]
10_Voirie_reseaux_divers	[10_VRD]
11_Ordre_public	[11_ORP]
12_Enfance_Jeunesse	[12_EJE]
13_Aide_sociale	[13_AIDSOC]
14_Agriculture	[14_AGRI]
15_Sante_&_Environnement	[15_SANENV]
16_Economie	[16_ECO]
17_Tourisme	[17_TOUR]
18_Culture	[18_CULT]
19_Sports	[19_SPO]
20_Associations	[20_ASSO]



NIVEAU 2 : un exemple

Construire une arborescence

01_Administration_generale

[01_ADGEN]

01_01_Courrier_Chrono

[CHRONO]

Depart
Arrivee
Plaintes_Petition
Cartes_de_vœux_reçues_Elus
Actes_deposes-en_mairie_Huissiers

01_02_Maire_Elu

[MAIRELUS]

Registre_arretes
Decisions_Maire
Agendas_Maire
Courrier_personnel_Maire

01_03_Conseil_municipal [CM]

Registre_deliberations
Dossier_preparation_Conseil
Dossier_seance_Conseil
Contrôle_de_legalite
Commissions_du_Conseil
Bureaux_Conseil
Recueil_des_actes_administratifs



Gestion de l'arborescence au quotidien

Construire une arborescence

- Établir un **document de référence validé** par la direction et régulièrement mis à jour
- Désigner un **responsable référent du plan de classement**
- Travailler régulièrement à l'élimination des documents inutiles ou doublons
- **Imposer et faire respecter une politique de droits d'accès** pour les utilisateurs (vigilance concernant certains dossiers sensibles)
- Vérifier la conformité au regard des **traitements de données personnelles**



Destruction / élimination de fichiers

Construire une arborescence

Les documents nativement électroniques et les documents numériques signés électroniquement ont la **même valeur que les archives papier** et ne peuvent pas être éliminés sans autorisation

⇔ **Obligation de rédiger un bordereau d'élimination**

⇔ **Validation par le directeur des Archives départementales**

Conseil

Procéder à un nettoyage (cleaning day) annuel

Fiche 3

Gérer et conserver ses fichiers numériques

Les données et documents électroniques produits ou reçus par une administration dans le cadre de son activité constituent des archives publiques et à ce titre, ils sont soumis au contrôle scientifique et technique de l'État.

Une bonne organisation permet :

- un gain de temps et d'espace
- de garantir l'accessibilité des documents et de faciliter la recherche
- d'éviter les pertes
- de garantir une bonne conservation



Attention ! L'archivage électronique ne doit pas être confondu avec la sauvegarde (fait de réaliser une copie de sécurité) ou le stockage (opération consistant à garder des données sur un support ou un espace dédié). L'archivage électronique conserve les données et en maintient l'accès à très long terme.

Construire et gérer son arborescence (ou plan de classement)

L'arborescence est un plan de classement des fichiers qui permet de ranger ses documents de manière structurée dans les espaces de stockage afin de les retrouver rapidement.

Le serveur doit être un lieu unique de stockage et de partage des documents du service, à l'exclusion des disques durs des agents (non sauvegardés) et des sessions personnelles (non partagées). Le serveur ne doit contenir aucun document privé.



Caractéristiques du plan de classement de l'arborescence du serveur :

- ▶ Inspirez-vous du plan de classement de vos documents papier.
- ▶ Identifiez les missions et hiérarchisez-les du général au particulier.
- ▶ Numérotez les premiers niveaux de l'arborescence.
- ▶ Choisissez des intitulés de dossiers explicites et compréhensibles par tous afin de faciliter la recherche.
- ▶ Limitez le nombre de niveaux à 3 maximum.
- ▶ Utilisez des raccourcis au lieu de copier le même fichier à deux endroits.

Voir aussi le modèle d'arborescence proposé (fiche séparée)

Quelques conseils

- Pensez à faire un bilan pour ajuster l'arborescence lors d'une réorganisation ou à chaque récolement post-électoral réglementaire.
- Une fois par an, vous pouvez consacrer un temps pour le nettoyage de l'arborescence.
- Harmonisez le nommage des fichiers dans chaque service pour une meilleure gestion au quotidien, et afin de les rendre utilisables sur le long terme.



Fiche 3

Règles de base de nommage

Formaliser une politique de nommage (archiviste/responsable de service/ correspondant...)

- ▶ Donner un nom unique, explicite, homogène pour le même objet, et court :
 - le placer en premier **Exemple : EgliseReparation.docx**
 - À noter : la longueur maximale de l'adresse complète du fichier ne doit pas excéder 256 caractères.
- ▶ L'ordre des mots est à choisir en fonction du type de classement utilisé :
 - chronologique
 - alphabétique
 - numérique...
- ▶ Pas d'espace, ni de caractères accentués ou spéciaux, ni d'accent : le **tiret bas** (underscore) ou les caractères en **majuscules** peuvent faire office de séparateur.
- ▶ Indiquer les **dates** au bon format
 - Le format recommandé par la norme internationale ISO 8601 est YYYY-MM-DD (year-month-day ou année-mois-jour) : <https://www.iso.org/fr/iso-8601-date-and-time-format.html>
- ▶ Indiquer les **versions** des documents **Exemple : Cr_ReunionPlieniére_V1.docx**
- ▶ Un document garde le **même nom** quel que soit son format
Exemple : Photo_mairie.jpeg ; Photo_mairie.pdf ; Photo_mairie.xls ; Photo_mairie.docx.



Adopter le bon format

- ▶ Les formats de fichiers sont nombreux et, du fait des évolutions fréquentes, peuvent devenir rapidement obsolètes.
- ▶ Privilégier les **formats libres, dits ouverts** : ils ne sont pas propres à une application accessible à tous (JPEG, TIFF, PDF...). Ces formats permettent la lisibilité sur le moyen et long terme.
- ▶ Les formats propriétaires, dits fermés (ex : .doc, .xls), peuvent poser des problèmes de lecture en cas de disparition d'un logiciel, d'un éditeur..., voire entraîner des pertes de données. Ils présentent donc plus de risques d'obsolescence :
- ▶ Il convient donc de privilégier les formats durables.
- ▶ En fonction des types de documents, les formats suivants sont recommandés : voir le référentiel général d'interopérabilité de l'État <https://www.numerique.gouv.fr/publications/interopabilite/>



Types	Format recommandé
Fichiers bureautiques	XML, PDF/PDF-A, TXT, ODF
Bases de données	XML, CSV, SIARD
Courriels	MBOX, EML
Images	JPEG, TIFF, PNG

- Identifier tous les documents numériques du service
- Appliquer les règles de nommage de fichier et adopter un plan de classement
- Insérer les métadonnées à chaque création de fichiers ou de dossiers
- Penser à alerter les Archives départementales en cas de changement de logiciel ou de perte de données
- Informer et demander l'autorisation des Archives départementales pour éliminer des données numériques

À retenir





Comité d'experts de la donnée du Tarn

Priorisation des données



*Yann LOGELIN
archiviste
Ville de Castres*



*Pierrick JEAY
Délégué à la Protection des Données
Communauté d'Agglomération de l'Albigeois*



Comité d'experts de la donnée du Tarn

La priorisation des données

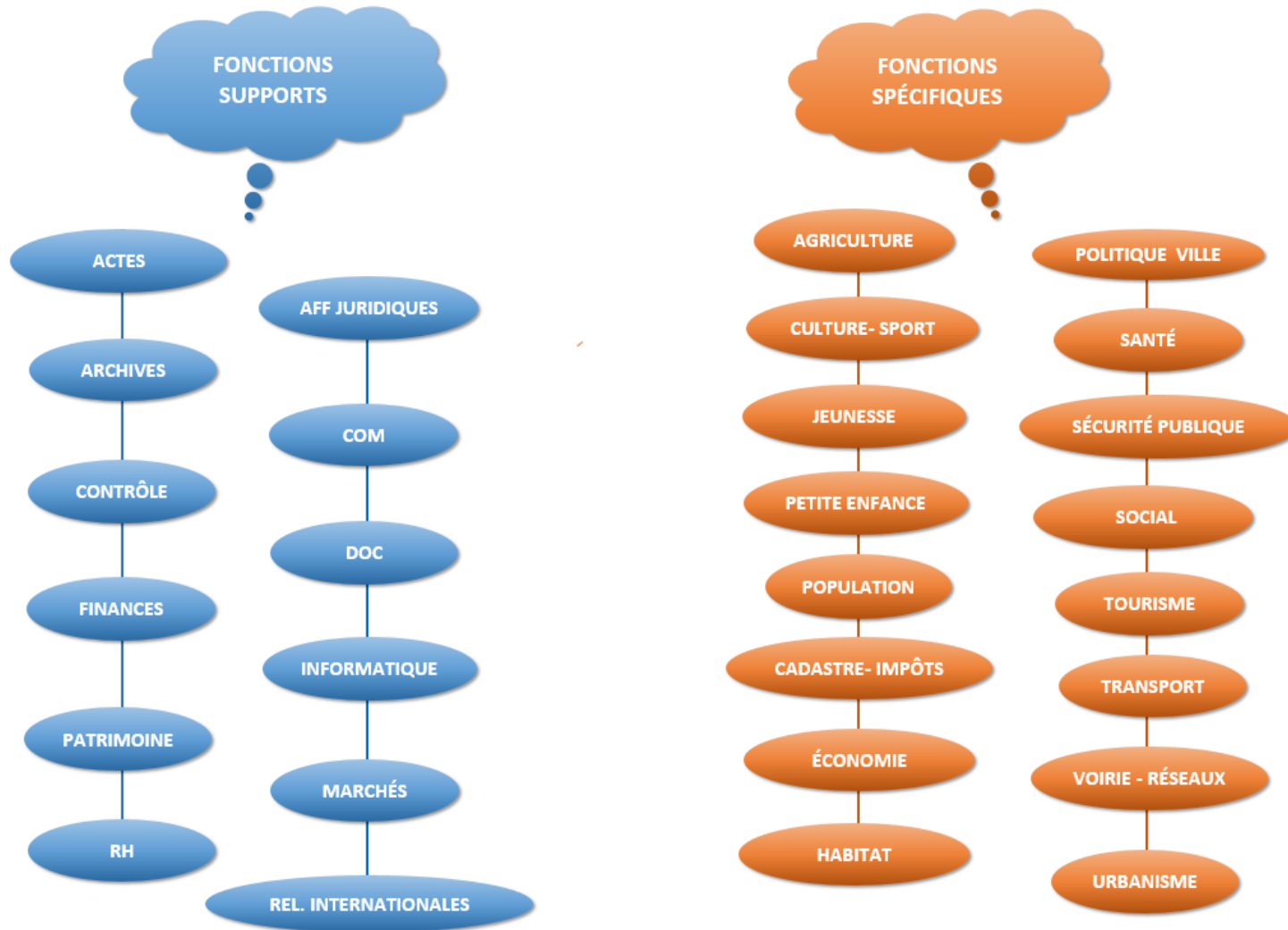
Ce groupe de travail propose un tableau qui définit pour chaque type de document produit par les communes, papier ou dématérialisés, la priorisation des données selon :

- Les fonctions supports de la municipalité, c'est-à-dire les données des instances de décisions (le conseil municipal par exemple) et les documents utiles au fonctionnement interne de la commune (informatique, finances etc.)
- Les fonctions spécialisées, c'est-à-dire les données des services au service de la population de la commune (action sociale, habitat, culture etc.).



Comité d'experts de la donnée du Tarn

Priorisation des données





Comité d'experts de la donnée du Tarn

La priorisation des données

Trois types de priorité ont été définis avec des couleurs associées :

- **Priorité 1** : concerne les données essentielles pour la prise de décision. Pour l'archivage, ils sont à conserver de façon prioritaire.
- **Priorité 2** : pour la gestion courante, ce sont des documents support indispensables à la prise de décision. Pour l'archivage, ils ont un intérêt statistique ou historique essentiel.
- **Priorité 3** : pour la gestion courante, ce sont les documents annexes qui ont une importance à court terme. Pour l'archivage, ce sont des documents importants à conserver mais qui ont une valeur juridique, statistique et historique moindre.



Comité d'experts de la donnée du Tarn

La priorisation des données

[Accès au tableau de la priorisation des données communales](#)



Exemple des marchés publics

Fonctions/ Missions et activités/ Processus	Typologie de documents	Priorité pour gestion courante et intermédiaire	Justification	Priorité pour archivage	Textes de référence
6. Marchés publics		Priorité 1		Priorité 1	
1. Études préalables	<ul style="list-style-type: none"> * Étude d'impact ; * Étude de faisabilité ; * Étude technique ; * Programme. * Avant-projet sommaire. * Avant-projet détaillé. 	Priorité 1		Priorité 1	
2. Publicité	<ul style="list-style-type: none"> * Dossier de consultation des entreprises (DCE) * Annonces légales (insertion au Moniteur, au BOAMP et au JOUE). 	Priorité 2		DUA 5 ANS	
3. Réception et examen des offres	<ul style="list-style-type: none"> *Retrait des dossiers : récépissé de retrait * Remise des dossiers : récépissé de dépôt ou accusé de réception ; * Liste des entreprises ayant retiré un dossier ; * Liste des candidatures ; * Commission d'ouverture des plis : convocations, procès-verbal ; * Rapport d'analyse des offres. 	Priorité 1	Fonctionnement par dossier. Documents engageants juridiquement pour la CT. Soigner la gestion de ces archives courantes et intermédiaires. Nécessité de sécuriser.	Priorité 1	
4. Attribution et notification	<ul style="list-style-type: none"> * Dossier de l'entreprise ; * Procès-verbal d'attribution ; * Notification : accusé de réception ; * Lettre de rejet 	Priorité 1		Priorité 1	
5. Exécution	<ul style="list-style-type: none"> * Ordres de service * Suivi technique : notes, rapports, comptes rendus, planning de travaux, plans d'exécution d'ouvrage, procès-verbaux de réception, photographies, correspondance * Suivi financier : mandats ou certificats de paiement, cautions bancaires et mainlevées de cautionnement, décompte général définitif, certificat pour solde. 	Priorité 1		Priorité 1	
6. Liste annuelle des marchés publics		Priorité 1		Priorité 1	



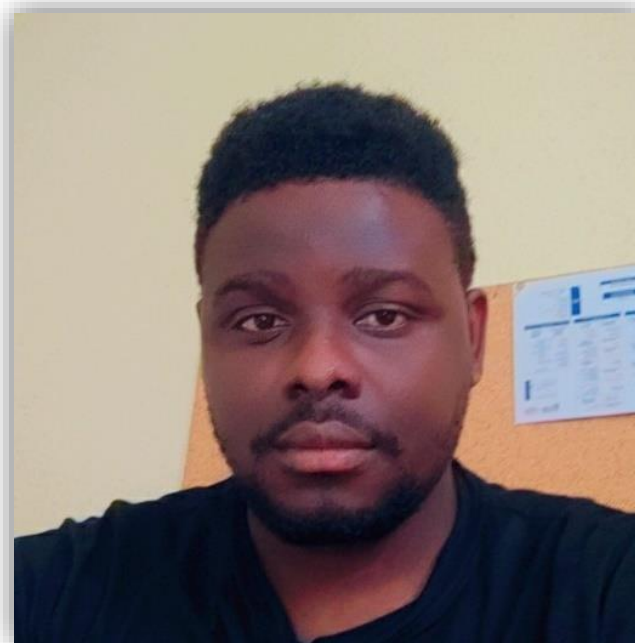
Comité d'experts de la donnée du Tarn

Cartographie de la donnée



Pierrick JEAY

*Délégué à la Protection des Données
Communauté d'Agglomération de l'Albigeois*



Christian Bah Leman

*Archiviste
Ville d'Albi*



Thèmes ciblés

Cartographie de la donnée

1. Matériel informatique
2. Bureautique
3. Mails
4. Numérisation
5. Sécurité et sauvegardes
6. Services
7. Formation et sensibilisation
8. Gestion des données et récolement
9. Logiciels
10. Usages numériques et contexte réglementaire

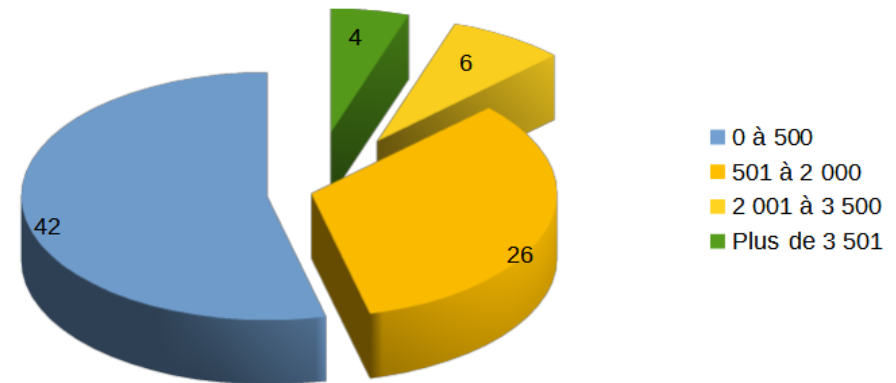


Panorama des répondants

Cartographie de la donnée

- **Nombre de réponses :**
 - 75 communes (24 %)
 - 3 EPCI sur 16
- **Utilisateurs et usages :**
 - 1 à 5 agents ou élus (communes)
 - Ordinateurs communaux

Taille en nombre d'habitants

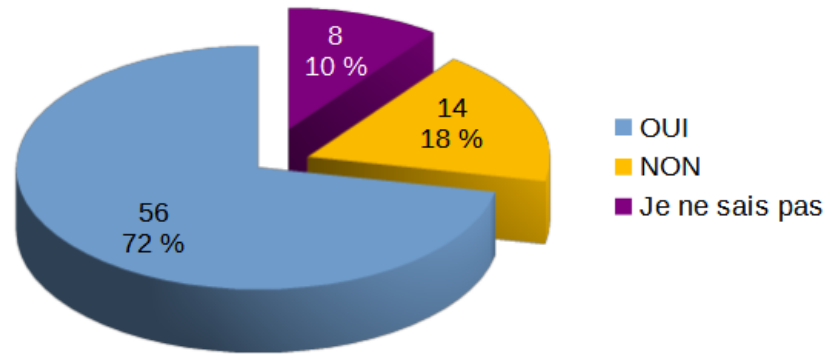




Gestion des e-mails

Cartographie de la donnée

Serveur de messagerie grand public

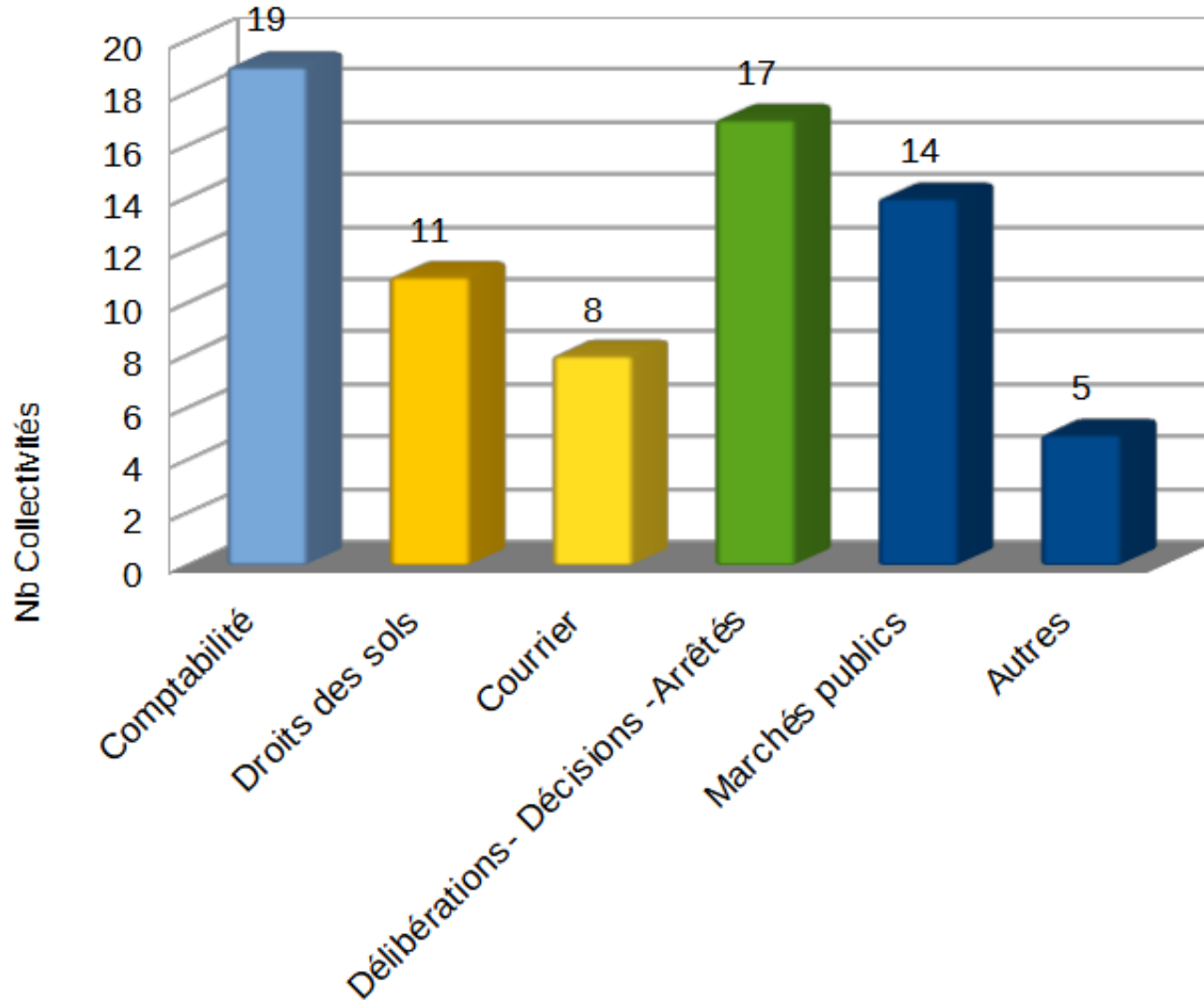


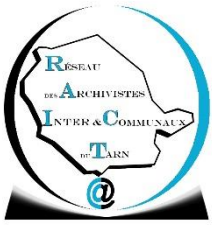
- **Points d'attention :**
 - Sécurité des échanges
 - Conformité au RGPD du service (GMail...)



Traitements dématérialisés

Cartographie de la donnée





Arborescence de fichiers

Cartographie de la donnée

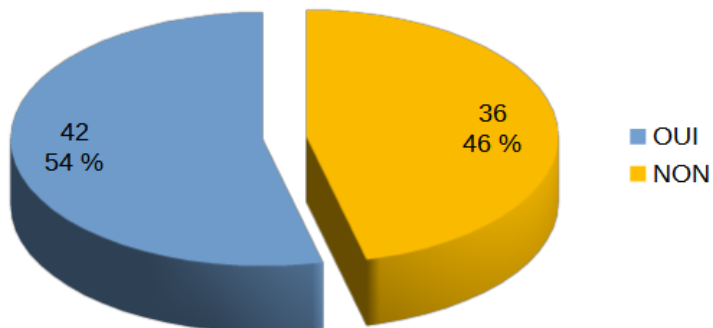
- **Questionnement sur la perception de l'arborescence de fichiers** (*le système de classement*)
- **L'arborescence :**
 - **Vous paraît-elle ordonnée ?**
 - **Est-elle documentée ?** (*avez-vous rédigé un « mode d'emploi »*)
 - **Vous paraît-elle fonctionnelle ?**
(*vous classez et retrouvez, en une minute environ, un document que vous avez produit*)
 - **A fait l'objet d'une révision, d'un meilleur plan de classement ?**



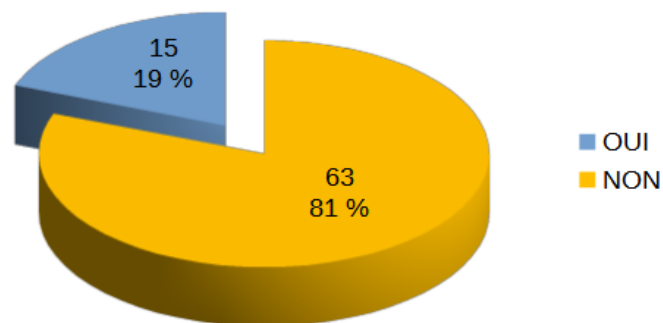
Arborescence de fichiers

Cartographie de la donnée

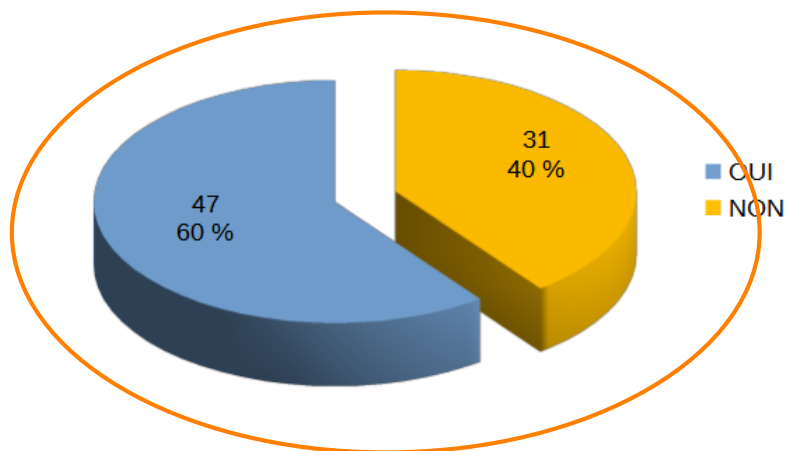
Arborescence ordonnée



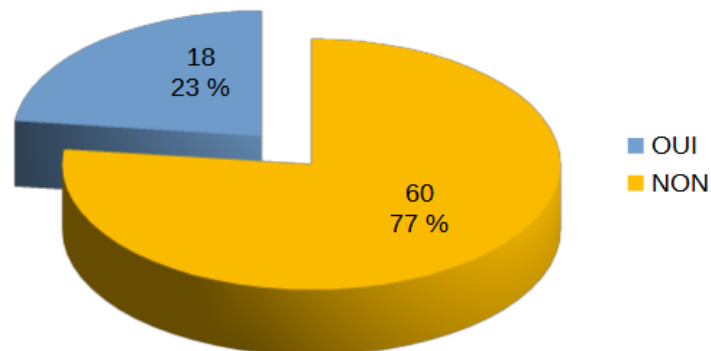
Arborescence documentée



Arborescence fonctionnelle



Arborescence révisée

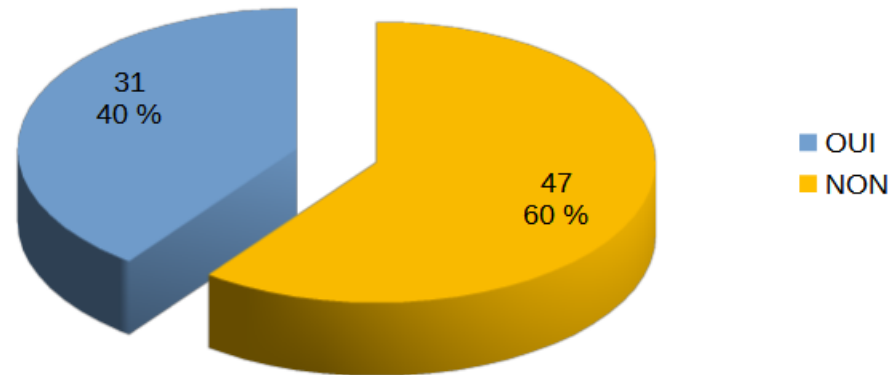




Usage d'un serveur de fichiers bureautiques

Cartographie de la donnée

- Part des communes disposant d'un serveur de fichiers bureautiques :

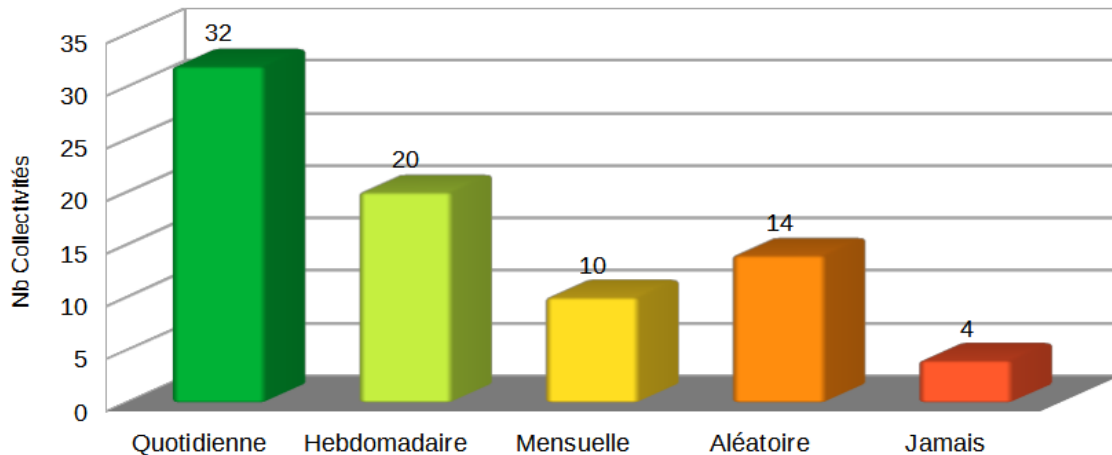




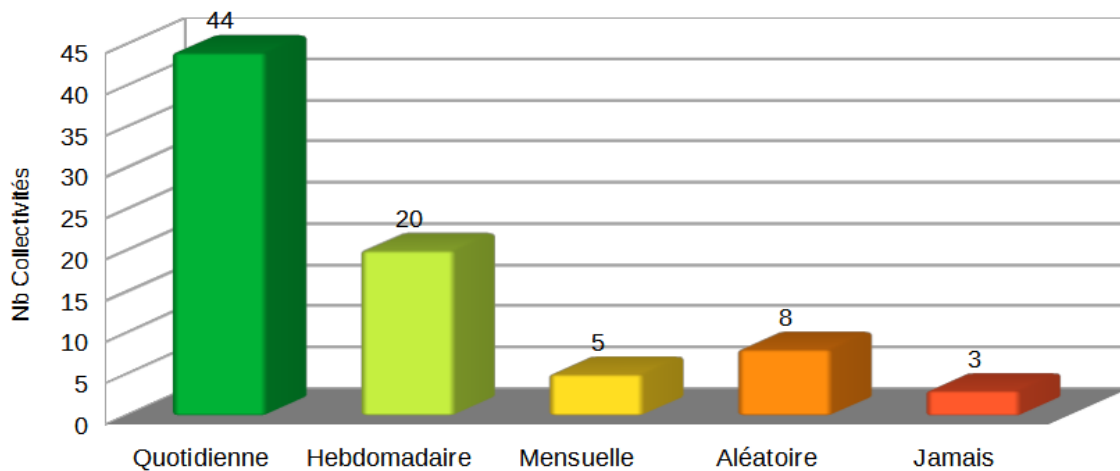
Gestion des sauvegardes

Cartographie de la donnée

Sauvegarde fichiers bureautique



Sauvegarde logiciels





Le délégué à la protection des données

Cartographie de la donnée

- **Avez-vous désigné un délégué à la protection des données ?**

(nombre de communes)

- **Oui : 48**
- **Non : 30**

Rappel : obligation réglementaire depuis le 25 mai 2018



Besoins en formation

Cartographie de la donnée

Êtes-vous demandeur de formation ou de sensibilisation dans le domaine de la :	
Dématérialisation des procédures	40
Gestion des archives	62
Protection des données	42
Sécurité informatique	46
Sauvegarde	38
Comment verriez-vous le format de la formation	
Court (2 heures)	45
Long (2 journées)	16
En présentiel	39
En <u>visio-conférence</u>	37
Avez-vous quelque chose à ajouter ?	
cela dépend des sujets à voir	
Durée de la formation à adapter selon le sujet	
formation arborescence rangement des fichiers	

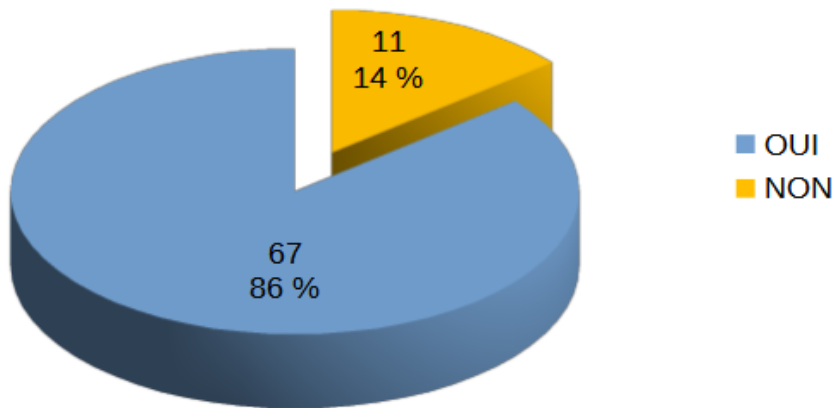


Besoins spécifiques

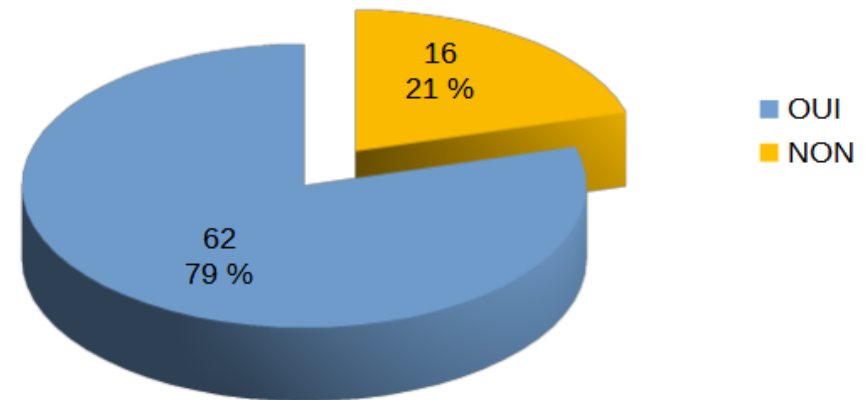
en matière d'archivage et de gestion des données

Cartographie de la donnée

Besoin en méthodologie archives numériques



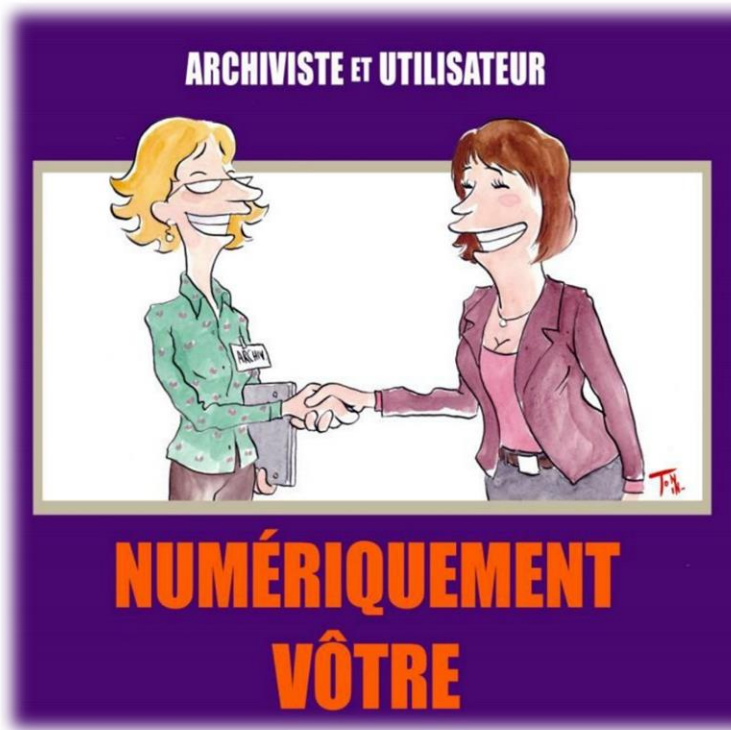
Besoin en méthodologie archives papier





Et maintenant....

Actions à mener et perspectives





Comité d'experts de la donnée du Tarn

Actions à mener

- Proposer des formations en s'appuyant sur les résultats de l'enquête
- Accompagner les collectivités locales dans la gestion de la donnée
- Instaurer des partenariats (groupe départemental des DPO, DSI...)
- Veille et diffusion de l'information



BILAN ET PERSPECTIVES

- Mise en place d'un SAE (système d'archivage électronique)
- Mise en place d'une mutualisation de l'archivage

Des questions

RGPD

archivage des mails

arborescence



SAE

cyber sécurité

gestion des mails

Contacts et ressources



Archives départementales
Comité d'experts de la donnée du Tarn
archives.tarn@tarn.fr



Association des maires du Tarn : *contact@maires81.asso.fr*



Centre de gestion du Tarn : *cdg81@cdg81.fr*

**Merci pour
votre attention**