Gérez vos documents électroniques
Fiche conseil n°5 - Conservez vos données et documents électroniques sur le long terme

Les données et documents électroniques produits ou reçus par une administration dans le cadre de son activité (courrier électronique, fichier bureautique, base de données, etc) sont des archives publiques.

Afin d'en garantir l'authenticité, l'intégrité et l'accessibilité sur le long terme, il est nécessaire de prendre en compte quelques règles.

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.

QUELS OBJECTIFS ?

- L'intégrité : caractéristique d'un document électronique qui n'a subi aucune destruction, altération ou modification.
- La lisibilité : possibilité, lors de la communication d'un document, d'avoir accès à l'ensemble des informations qu'il comporte.
- L'authenticité : caractère d'un document dont on peut prouver qu'il est bien ce qu'il prétend être (fiabilité du contenu, de la date, du producteur et du contexte de production). La signature électronique garantit l'identité du signataire et l'intégrité du document signé, et protège la confidentialité des informations.
- La traçabilité : fait de créer, d'enregistrer et de préserver des données relatives à l'utilisation des documents.
- La pérennité : capacité à garantir l'intégrité, la lisibilité et l'authenticité des objets archivés sur une longue durée.

Notons qu'il existe des systèmes d'archivage électronique (SAE) qui associent des outils et des procédures permettant d'atteindre ces objectifs, notamment :

- L'intégrité, par la vérification régulière de l'empreinte numérique du document.
- La traçabilité, par la mention horodatée dans le journal de cycle de vie des archives de l'ensemble des actions effectuées sur un document (versement, communication, élimination, vérifications diverses...). Ce journal est régulièrement archivé comme n'importe quel document.

A défaut d'un tel système, il est possible de mettre en œuvre de bonnes pratiques.

QUELS OUTILS ?

- Renseigner les métadonnées

- Les métadonnées :
  - Sont des informations sur le contenu (date, auteur, légende, mots-clés, champs d'une base de données, etc) et des informations techniques (format, structure et codification des données, propriétés du fichier, indications sur l'environnement logiciel, matériel nécessaire à la lecture, droit d'accès, etc) décrivant des documents électroniques.
  - Permettent d'en contextualiser la création, d'en faciliter la gestion et l'exploitation.
  - Une partie de ces informations peut être enregistrée automatiquement dans les « propriétés du document ».
- À défaut, il est important de créer, dans le titre du document ou dans un en-tête créé à cet effet, des métadonnées de contenu : nom de l'auteur, date de création, date de mise à jour, nom du destinataire, version, nom du projet.

- Choisir des formats adaptés à la conservation

- Les formats de fichiers sont nombreux et, du fait des évolutions fréquentes, peuvent devenir rapidement obsolètes.
- Les **formats libres, dits ouverts**, se caractérisent par des spécifications accessibles à tous (ex : PDF, JPEG). Ces formats ne sont donc pas propres à une application. Le caractère « ouvert » d'un format est un atout pour en permettre la lisibilité sur le moyen et long terme.
- Ils s'opposent en cela aux formats propriétaires, dits fermés (ex : .doc, .xls), qui 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 : la compatibilité entre deux versions d'un logiciel peut être rompue en moins de 10 ans. Une conversion vers un format ouvert sera alors recommandée avant tout archivage définitif.
- 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'Etat. http://references.modernisation.gouv.fr) :

Type de document	Format recommandé
Fichiers bureautiques	XML, PDF/PDF-A, TXT, ODF
Courriels	MBOX, EML
Bases de données	XML, CSV, SIARD
Images	JPEG, TIFF, PNG
Plans vectoriels	CGM, DXF, PDF/A-2
Sons	MP3, WAV, FLAC
Audiovisuel	MPEG-4

- Choisir des supports fiables

- Quels qu'ils soient, les différents supports existants ne présentent pas tous les garanties pour une conservation sur le long terme (disque dur, CD-ROM, clé USB, *etc.*) : leur durée de vie est en général de 5 à 10 ans.
- Ces supports sont également sensibles à divers facteurs de dégradation (usure, conditions de stockage, instabilité des matériaux, erreurs humaines…).
- Il convient donc :
  - de sélectionner des produits normalisés, robustes, résistants aux agressions de l'environnement et vieillissant lentement ;
  - d'envisager des migrations régulières vers de nouveaux supports pour les données à longue durée de conservation.
- Malgré cela, même si un support est bien conservé et ne connaît pas de dégradations, il sera confronté à terme à l'obsolescence des matériels de lecture.
- Attention : il est interdit pour une administration produisant des archives publiques de souscrire à une offre de *cloud* dont le prestataire ne peut garantir que l'ensemble des traitements et de l'hébergement des données sont effectués sur le territoire français.

- Sécuriser ses équipements et réseaux

- Conserver les données sur 2 supports distincts et diversifiés (serveurs, bandes magnétiques, disques optiques, *etc.*), situés sur 2 sites différents, éloignés l'un de l'autre, et placés en « miroir » : en cas de panne de l'un, les données seront préservées sur l'autre.
- Protéger les salles des serveurs contre l'incendie, les inondations, les pannes électriques, la poussière, la surchauffe.
- Procéder à des migrations régulières (tous les 5 ans si possible) : transfert des données sur de nouveaux supports (baies, disques durs, CD, *etc.*), et ce sous des formats durables afin d'en garantir la conservation et la communication.
- Sécuriser l'accès aux serveurs : accès physique (habilitations restreintes, enregistrement), accès informatique (antivirus, pare-feu, journal des événements).
- Sécuriser l'accès aux données par la mise en œuvre d'un système d'authentification (gestion des droits d'accès aux applications, aux espaces serveurs, conservation des listes d'utilisateurs, *etc.*).

Nous contacter : Archives départementales du Loiret – 02 36 99 25 00 – dad@loiret.fr
Plus de renseignements sur www.archives-loiret.fr/administrations