

LIVRE BLANC



**EN ROUTE VERS
L'ARCHIVAGE ELECTRONIQUE
ET VOUS, VOUS FAITES QUOI POUR
VOS DOCUMENTS NUMERIQUES ?**

LOGARCHIVES

SOMMAIRE

| | |
|--|----|
| 1. Introduction | 3 |
| 2. Cloud, Archivage Electronique, GED, Coffre-fort... de quoi parle-ton ?..... | 5 |
| 3. Quelles exigences prendre en compte pour bien archiver vos documents électroniques..... | 9 |
| 4. Les bonnes raisons d'externaliser l'archivage électronique..... | 16 |
| 5. Les critères à prendre en compte pour choisir votre solution | 19 |

1. Introduction

L'année 2016 aura été très favorable au développement de la dématérialisation :

- **loi Macron** sur la généralisation de la dématérialisation des factures dans le public,
- **loi El Khomri** favorisant le bulletin de paye électronique,
- **règlement européen eIDAS** (Electronic Identification and Services) qui vise à promouvoir les services de confiance relatifs à l'identité numérique : horodatage, signature et cachet électroniques, lettre recommandée... afin de favoriser la dématérialisation des échanges dans toute l'Europe,
- **réforme du Code Civil sur la force probante de la copie numérique fidèle**, dont la mise en application est prévue début 2017. La copie numérique aura valeur probante sous réserve qu'elle soit **produite via des procédés spécifiques de numérisation** préservant la vocation probatoire du document et **conservée dans un système d'archivage pérenne**, c'est-à-dire un Système d'Archivage Electronique (SAE) à vocation probatoire tel que défini par la norme NF Z 42-013.

Face à la déferlante de documents numériques, dématérialisés, portant pour beaucoup une valeur juridique et des obligations de conservation, se pose la question des conditions de leur archivage.

Le marché propose de très nombreuses solutions : du nuage au logiciel de GED, en passant par le coffre-fort, la sauvegarde informatique... Pour autant, toutes ne répondent pas au même besoin, et à moins d'être un spécialiste, il est de plus en plus difficile de savoir « qui fait quoi ».

Mais avant de choisir votre solution, commencez par le commencement en répondant à ces questions :

- **Quels documents voulez-vous conserver ?** S'agit-il de documents nativement électroniques, ou de documents numérisés ? Dans le dernier cas, avez-vous utilisé un process de numérisation « simple » ou certifié NF Z 42-013 à vocation probatoire ?
- **Quels sont leurs enjeux respectifs ?** S'agit-il de documents engageants pour votre entreprise, présentant une sensibilité particulière (confidentialité...) ou à vocation probatoire ? Ou de documents nécessaires à votre activité quotidienne mais ne présentant pas de caractère critique ?

Quelques exemples pour illustrer le propos :

- les **bulletins de paye, factures, contrats dématérialisés** et signés électroniquement vous engagent fortement et nécessitent des conditions de conservation hautement sécurisées,
- dans un **dossier du personnel de crédit, un dossier immobilier...** le contrat n'a pas la même valeur que les pièces justificatives qui l'accompagnent,
- pour un laboratoire pharmaceutique, les **dossiers de lots de fabrication** doivent être consultables 24/24h et 7/7j en cas d'inspection des autorités de santé ou d'incident avec un patient. Leur numérisation NF Z 42-013 permet de disposer d'une copie fidèle accessible à tout moment pendant toute la durée de commercialisation du médicament,

- **Les dossiers techniques dans l'aéronautique, les brevets...** présentent eux aussi des enjeux forts pour les entreprises qui les détiennent.

Il existe des solutions de conservation adaptées pour chaque profil de documents.

C'est pour vous aider à décrypter les principales notions clés de l'archivage électronique que nous vous proposons ce livre blanc.

2. Cloud, Archivage Electronique, GED, Coffre-fort... de quoi parle-ton ?

Toute entreprise qui souhaite gérer ses documents électroniques se retrouve dans l'embarras du choix face à la diversité des solutions existantes sur le marché : cloud, coffre-fort numérique, sauvegarde informatique, stockage, hébergement, archivage électronique à vocation probatoire, GED...

Ces termes couramment utilisés peuvent recouvrir des réalités différentes selon les interlocuteurs. Par ailleurs, ces solutions ne sont pas équivalentes et répondent à des besoins informationnels différents.



COMMENT CHOISIR VOTRE SOLUTION ? PARTEZ DE VOTRE BESOIN ET DE VOS DOCUMENTS

Plutôt que de passer en revue les solutions proposées par les prestataires, il est préférable de commencer par bien définir vos attentes.

Vous pouvez vous appuyer sur une grille d'analyse pour déterminer vos besoins en matière de systèmes d'information, en **vous inspirant des notions "DCIP" (Disponibilité - Confidentialité - Intégrité - Pérennité) telles que définies dans la norme ISO 27001 afin de prioriser vos besoins :**

- **DISPONIBILITE** : les collaborateurs ont-ils besoin d'accéder souvent et rapidement aux documents ?
- **CONFIDENTIALITE** : quel collaborateur peut accéder à quels documents ?
- **INTEGRITE** : dans quelle mesure ces documents peuvent-ils être utilisés au titre de la preuve ?
- **PERENNITE** : est-il nécessaire de conserver les documents à long terme, voire parfois à très long terme ?

QUELLE SOLUTION TECHNIQUE POUR QUEL USAGE ?

Une fois les priorités de l'entreprise bien identifiées, il devient plus aisé de choisir parmi les solutions techniques existantes.

LE CLOUD : partager facilement les documents

Cette infrastructure mutualisée met à disposition d'un grand nombre d'utilisateurs des capacités de stockage, de télécommunication et de calcul. Principalement dédiée au partage, elle n'offre pas des garanties de sécurité optimales, même après ajout d'une couche de chiffrement. De plus, la localisation concrète des documents (et de leurs copies de sauvegarde) est incertaine : sont-ils stockés en France... ou ailleurs dans les nuages ?

LA SAUVEGARDE INFORMATIQUE : conserver une copie des données / applications à un instant T

Ce dispositif matériel et logiciel vise à disposer d'une copie des données et applications. Son rôle n'est pas de garantir la confidentialité et l'intégrité des documents, ni de naviguer ou de contrôler les accès aux documents. Il permet de restaurer votre système informatique en cas de perte ou de sinistre afin de poursuivre votre activité.

L'HEBERGEMENT : déléguer le stockage des documents à un tiers

Ce dispositif technique consiste à externaliser auprès d'un prestataire le stockage des documents, et de bénéficier d'une solution - plus ou moins sécurisée - à un bon rapport qualité / prix. Avec l'avantage de rester centré sur son cœur de métier et de ne pas gérer cette partie informatique.

LE COFFRE-FORT NUMERIQUE : protéger les documents et démontrer leur intégrité

Cette solution logicielle n'intègre pas les infrastructures techniques (firewall, serveurs dédiés...) indispensables pour garantir la pérennité et la disponibilité des documents.

LA GESTION ELECTRONIQUE DES DOCUMENTS (GED) : faciliter le travail collaboratif

Cet ensemble logiciel sert à décrire des documents vivants pour faciliter leur classement, leur modification et leur évolution pendant leur production, et permettre d'y accéder facilement pour les exploiter. Il n'a pas vocation à protéger l'intégrité d'un document ni d'assurer sa pérennité.

L'ARCHIVAGE ELECTRONIQUE A VOCATION PROBATOIRE : être capable d'apporter la preuve

Service plus qu'outil, un système d'archivage électronique (SAE) a pour rôle d'assurer la conservation à très long terme des documents et permet de garantir leur non-altération, en empêchant toute falsification volontaire ou involontaire.

EN CONCLUSION : grâce à la combinaison de briques logicielles et matérielles, de processus et d'interventions humaines, le Système d'Archivage Electronique constitue la seule solution capable de garantir simultanément la disponibilité, la confidentialité, l'intégrité et la pérennité des documents, et donc le maintien de leur vocation probatoire. Un SAE est de plus parfaitement complémentaire à un outil de GED.

FOCUS ARCHIVAGE ELECTRONIQUE ET GESTION ELECTRONIQUE DES DOCUMENTS

La Gestion Electronique des Documents (GED) et le Système d'Archivage Electronique (SAE) présentent des ressemblances, au point d'être souvent confondus.

Pourtant leurs finalités et leurs fonctionnalités sont fondamentalement différentes.

Plutôt que de les opposer, **il est nécessaire de réfléchir à leur complémentarité, source d'une gestion efficace de l'information dans l'entreprise.**

LE TOP 3 DES IDEES RECUES SUR LA GED ET LE SAE

Idée reçue n° 1 : la GED et le SAE, c'est la même chose : un seul outil suffit

FAUX ! Certes, l'usage qui en est fait et l'expérience utilisateur qui est proposée sont souvent semblables : on se connecte à un outil de recherche afin de trouver un document électronique. Pourtant les back office d'une GED et d'un SAE n'ont rien à voir... tout comme leurs finalités et leurs fonctionnalités !

Idée reçue n° 2 : je n'ai pas besoin d'un SAE pour sauvegarder mes documents importants.

FAUX ! Seul un Système d'Archivage Electronique est à même de fournir un environnement physique et informatique sécurisé garantissant l'intégrité et la pérennité des documents probants de l'entreprise. Aucune GED ne pourra remplir cette mission. Or, ne pas pouvoir apporter la preuve, c'est faire courir des risques juridiques et financiers à l'entreprise.

Idée reçue n° 3 : une GED va compliquer ma recherche d'informations.

FAUX ! La finalité d'une GED est justement de permettre d'accéder facilement et rapidement au document recherché... Une GED bien conçue facilitera donc les recherches des collaborateurs, sans accroître la complexité de la procédure d'accès aux documents.

| QUI FAIT QUOI ? | GESTION ÉLECTRONIQUES DES DOCUMENTS | SYSTÈME D'ARCHIVAGE ÉLECTRONIQUE |
|--|--|---|
|  DÉFINITION | Système de gestion de l'information permettant de décrire et classer des documents | Système de conservation de l'information permettant de garantir la disponibilité, confidentialité, l'intégrité et la pérennité des documents |
|  FINALITÉ | Faciliter le PARTAGE de l'information | Garantir la CONFIANCE dans les documents |
|  USAGE | Gestion quotidienne des documents pour la conduite des affaires | Conservation sécurisée des documents probants |
|  FORME | Simple logiciel installé sur n'importe quel poste informatique et système d'exploitation | Système informatique : - Respectant des normes (NF Z 42-013, ISO 461) - Comprenant un logiciel, des baies de stockage et un environnement logique (calcul d'empreinte, jetons d'horodatage...) et physique sécurisé |
| FONCTIONNALITÉS AUTORISÉES | GED | SAE |
| MODIFIER UN DOCUMENT | ✓ | ✗ |
| FAIRE COEXISTER PLUSIEURS VERSIONS | ✓ | ✗ |
| DÉTRUIRE UN DOCUMENT | ✓ | ✗ sauf gestion du sort final |
| GÉRER DES RÈGLES DE CONSERVATION | parfois | ✓ |
| DÉFINIR UNE STRUCTURE DE CLASSEMENT | parfois - gérée par les utilisateurs | ✓ centralisée par l'Administrateur |

EN CONCLUSION : pour faire le bon choix, il est important de toujours conserver à l'esprit l'objectif principal de votre projet : voulez-vous avant tout accompagner la mobilité de vos collaborateurs ? Protéger vos documents sensibles ? Les retrouver facilement ? Apporter la preuve ? Par ailleurs, il ne faut pas hésiter à réviser votre projet en fonction des possibilités techniques et des coûts afférents.

3. Quelles exigences prendre en compte pour bien archiver vos documents électroniques

L'essor de la dématérialisation et de l'archivage électronique contribue à développer et valoriser le patrimoine informationnel des entreprises.

Grâce aux solutions de gestion et d'archivage électronique, les collaborateurs ont plus facilement accès à un important volume d'informations bien référencées.

Si cette richesse informationnelle permet de gagner en efficacité, elle accroît également les risques de divulgation et de corruption de vos données, ce qui est particulièrement problématique en cas de documents engageants pour l'entreprise.



2.1 DISPONIBILITE ET CONFIDENTIALITE

Définissez vos besoins de disponibilité et de confidentialité : **un audit préalable à la mise en place d'une politique d'archivage électronique permettra d'identifier les risques encourus ainsi que vos attentes par rapport au système d'archivage.**

Il peut être utile de s'appuyer sur les notions de disponibilité et de confidentialité, issues de la norme ISO 27 001.

2.1.1 LA DISPONIBILITE : DANS QUEL DELAI VOS COLLABORATEURS ONT-ILS BESOIN D'ACCEDER AUX DOCUMENTS ?

Pour être exploitable, un document électronique doit être accessible. Reste à savoir dans quel délai. Celui-ci étant fonction du métier de chaque entreprise, il est indispensable d'analyser les exigences opérationnelles de vos collaborateurs.

- **BIEN EVALUER VOS BESOINS :** la digitalisation massive contribue à fausser la perception des besoins réels. « **Puisque c'est informatisé, je dois pouvoir accéder tout de suite à mon document !** ». Mais l'utilisateur en a-t-il réellement besoin "tout de suite", ou peut-il attendre ?

Exemple : un service RH peut avoir besoin d'accéder à des dossiers du personnel dans un délai d'1 à 2 jours ouvrables. Dans ce cas, le recours à l'archivage numérique n'est pas nécessaire, un archivage papier performant répondra très bien aux besoins.

- **DEFINIR VOTRE BESOIN DE FONCTION DE VOS RISQUES** : l'exigence de disponibilité doit être définie en fonction des risques encourus si vous ne pouvez disposer du document dans le délai fixé.

Exemple : un laboratoire pharmaceutique américain doit pouvoir fournir instantanément, c'est-à-dire 24 heures sur 24 et 7 jours sur 7, en temps réel, ses dossiers de production à la Food and Drug Administration (FDA). Dans le cas contraire, il risque de perdre son accréditation à distribuer ses produits, avec un impact direct et très important sur son chiffre d'affaires, voire son activité.

2.1.2 LA CONFIDENTIALITE : QUI A DROIT D'ACCEDER A VOS DOCUMENTS ?

Gérer la confidentialité permet de limiter l'accès d'un document aux seuls utilisateurs autorisés, de gérer leurs droits d'usage et de mémoriser l'utilisation qu'ils en ont fait. Question à se poser : quels collaborateurs peuvent accéder à quels documents, et pour quoi faire ?

- **ANALYSER LE RISQUE LIE AUX DOCUMENTS** : la confidentialité est étroitement liée à la disponibilité. Certains documents sont forcément plus ou moins confidentiels. Il est donc impossible de donner à des personnes la possibilité de consulter un document sans établir en même temps un contrôle sur ce droit de consultation.

D'autre part, le passage à l'électronique génère des craintes et accroît des attentes en termes de confidentialité. "Et si un hacker mal intentionné s'emparait de mes fiches de paie ?". Le risque et ses éventuelles conséquences doivent être évalués à leur juste mesure.

- **ANALYSER LA CRITICITE DE VOS DOCUMENTS EN FONCTION DE CHAQUE METIER** : il faut repartir de l'analyse de votre métier, de l'éventuelle criticité de vos informations, de la taille de votre entreprise et de votre organisation.

Le périmètre d'accès aux informations peut être organisé par typologies de documents, en fonction des métiers. Dans une petite entreprise ne travaillant pas dans un domaine stratégique, on peut envisager une organisation simple de la confidentialité par métier. Tous les contrats commerciaux seront accessibles à l'ensemble de l'équipe commerciale, toutes les factures à la comptabilité, toutes les fiches de paie au service RH...

Il est bien sûr possible d'établir des règles d'accès beaucoup plus complexes, en attribuant à chaque document sa propre règle de confidentialité, encapsulée dans une métadonnée. Pour un laboratoire de R&D, seule la personne qui a créé le document et son supérieur hiérarchique pourront y accéder.

EN CONCLUSION : pour être complet, tout projet de dématérialisation doit intégrer une réflexion sur les moyens à mettre en œuvre pour conserver les documents en bout de chaîne, et donc l'archivage électronique.

2.2 INTEGRITE

Enjeu capital pour les entreprises, l'intégrité vise à minimiser leur risque juridique en cas de recours devant un tribunal, en s'assurant que leurs documents ne seront pas contestés par le juge.

Préserver l'intégrité d'un document nécessite de pouvoir démontrer qu'il n'a pas été corrompu, de manière volontaire ou involontaire.

La nature immatérielle et intangible de l'environnement numérique induit une défiance, qui renforce l'exigence d'intégrité pour les documents électroniques. C'est pourquoi il est nécessaire de mettre en œuvre des dispositifs supplémentaires venant renforcer la confiance.

Prenons l'exemple d'une entreprise ayant un contentieux avec un client à propos d'une facture :

- Cas n° 1 : la facture originale est émise au format papier. Cette facture n'a pas besoin d'être signée, le document se suffit à lui-même et sera accepté par le juge au titre de la preuve, sauf cas particulier,
- Cas n° 2 : la facture originale est émise au format électronique, par exemple en PDF. Pour constituer une preuve non contestable, le fichier PDF doit au minimum être accompagné d'une signature électronique de type RGS ⁽¹⁾ qui intègre notamment un calcul d'empreinte, ou d'une piste d'audit.

(1) certificat de signature répondant à des exigences techniques minimales

2.2.1 LA NORME NF Z 42-013 AU SECOURS DE LA PREUVE NUMERIQUE

C'est pour répondre à ce besoin que la norme NF Z 42-013 a été créée en 2013. Elle fixe les exigences techniques et organisationnelles requises pour :

- la conservation des archives électroniques et la préservation de l'intégrité,
- le cas échéant, la maîtrise du processus de numérisation permettant de constituer des copies fidèles à l'original et durables.

Choisir de mettre en oeuvre un Système d'Archivage Electronique (SAE) certifié NF Z 42-013 selon les règles NF 461, c'est faire le choix :

- d'un dispositif qui renforce la confiance numérique : conception du SAE, fiabilité des documents, sécurité et pérennité des infrastructures...,
- d'un niveau de protection optimal contre d'éventuels risques de falsification... et donc les risques juridiques associés,
- de la confiance attribuée par le tiers indépendant qui a réalisé l'audit.

FOCUS : L'EMPREINTE AU SERVICE DE LA PRESERVATION DE L'INTEGRITE D'UN DOCUMENT NUMERIQUE

Pour appliquer la norme NF Z 42-013, on recourt à un mécanisme cryptographique : le calcul d'empreinte, associé à la journalisation de cette empreinte.

Cette opération mathématique consiste à calculer l'empreinte numérique unique pour chaque document, équivalente à l'empreinte digitale, elle aussi unique pour chaque personne.

L'empreinte est ensuite conservée dans un journal afin de pouvoir tracer les éventuelles modifications ultérieures.

Le développement des nouvelles technologies a entraîné le développement de nouvelles compétences... aujourd'hui, falsifier un document Word ou PDF est (presque) à la portée du premier venu.

L'entreprise doit donc se préserver d'attaques de toutes sortes : de la simple erreur d'un collaborateur à l'acte de malveillance.

LES 4 NIVEAUX DE PROTECTION DE L'INTEGRITE D'UN DOCUMENT NUMERIQUE : L'EXEMPLE DE LA FACTURE

NIVEAU 1 : CALCUL DE L'EMPREINTE NUMERIQUE DE LA FACTURE



NIVEAU 2 : CREATION D'UN LOG DE L'EMPREINTE ET STOCKAGE DANS UNE BASE DE JOURNALISATION



NIVEAU 3 : CREATION D'UN JOURNAL DES LOGS



NIVEAU 4 : CALCUL DE L'EMPREINTE DU JOURNAL, SCÉLÈMEMENT ET VERSEMENT DANS UN SYSTÈME D'ARCHIVAGE ÉLECTRONIQUE



EN CONCLUSION : *il revient à l'entreprise d'analyser le type de risque encouru en fonction des différentes typologies de documents, et de choisir la solution adaptée. Un Système d'Archivage Electronique certifié NF Z 42-013 offre sans aucun doute le plus fort niveau de protection.*

2.3 PERENNITE

Le développement des nouvelles technologies a permis aux entreprises de s'affranchir des contraintes du papier en dématérialisant leurs flux de documents, générant ainsi un nouveau défi : maintenir la pérennité des archives électroniques, c'est-à-dire la capacité à conserver des données sur une longue durée.

2.3.1 LES DONNEES NUMERIQUES SONT VOLATILES

Un support papier conservé dans de bonnes conditions est par nature pérenne. Son contenu restera intelligible au cours des siècles et, même s'il subit une dégradation, la majeure partie des informations pourront être sauvées. A contrario, un fichier électronique est bien plus volatile du fait de son format :

- il est impossible d'accéder aux données du fichier si le format n'est pas adapté au logiciel, au système d'exploitation et à l'ordinateur,
- il n'existe aucune normalisation des formats de fichiers (excepté le pdf et le xml),
- la lisibilité d'un fichier dépend donc du bon vouloir de l'éditeur du logiciel qui peut faire défaut (faillite de l'entreprise, arrêt d'un logiciel) ou imposer des sauts technologiques (obligation d'acheter la nouvelle version du logiciel),
- un fichier corrompu devient le plus souvent illisible, et la reconstitution des données perdues s'avère coûteuse voire impossible.

De plus les supports utilisés (CD ROM, disques durs, serveurs informatiques...) sont fragiles et ont une durée de vie limitée.

Le cycle de vie très court des supports et formats électroniques ne coïncident pas avec les durées légales d'archivage des documents, qui peuvent aller de 10 ans pour une facture à 30 ans (contrat de travail) et plus (conservation pendant toute la vie du patient de son dossier médical, parfois même au-delà).

L'entreprise qui souhaite conserver les données d'un document numérique devra donc au moins une fois - et sans doute beaucoup plus - le convertir dans un autre format et faire migrer son hébergement sur un autre support de stockage.

2.3.2 LA PERENNITE DES DOCUMENTS NUMERIQUES : UN ENJEU CAPITAL POUR LES ENTREPRISES

Il est vital pour une entreprise de disposer des informations nécessaires à la bonne conduite de son activité, pour faire valoir ses droits en cas de contentieux et pour répondre à ses obligations légales de conservation des archives.

Depuis 2010, les cas d'entreprises n'ayant pas anticipé les enjeux de la pérennité de leurs archives électroniques et restées prisonnières d'un format de fichier propriétaire se sont multipliés.

Dans certains cas, l'entreprise a été obligée de conserver des ordinateurs antédiluviens, équipés d'anciennes versions du logiciel et du système d'exploitation afin d'accéder aux données de ses fichiers. Dans les pires scénarios, l'entreprise a perdu la majeure partie de ses données après avoir omis de procéder à des mises à jour régulières de son logiciel.

Comment éviter d'en arriver là ?

5 CONSEILS POUR ACCROITRE LA PERENNITE DE VOS ARCHIVES ELECTRONIQUES

| | |
|---|---|
| 1 | Enregistrer vos documents dans un format de fichier durable et normalisé , comme par exemple le PDF |
| 2 | Convertir régulièrement vos fichiers dans un format plus récent afin de prolonger leur lisibilité |
| 3 | A chaque conversion de fichier, vérifier un à un que les nouveaux fichiers créés sont conformes aux originaux afin de garantir leur intégrité et recalculer leur empreinte pour enregistrer la conversion réalisée |
| 4 | Disposer de serveurs redondés afin d'éviter la perte de données et de documents en cas de panne du matériel |
| 5 | Migrer régulièrement vos données et documents sur un nouveau serveur |

Ces opérations de conversion et de migration nécessitent des moyens importants tant sur le plan matériel qu'humain. Leur coût est proportionnel au nombre de documents à pérenniser et à la durée de conservation, et peut donc rapidement s'avérer élevé pour l'entreprise.

D'où l'intérêt de mutualiser ces coûts avec d'autres entreprises en recourant aux services d'un tiers archiveur, dans le cadre d'un Système d'Archivage Electronique à vocation probatoire.

EN CONCLUSION : QUELLES OPTIONS POUR GARANTIR LA PERENNITE DE VOS DOCUMENTS ELECTRONIQUES ? L'entreprise doit rester consciente des risques induits par l'électronique, et donc se donner les moyens de garantir la pérennité (et l'intégrité) de ses archives numériques. Ces deux notions sont étroitement liées : quel intérêt y aurait-il à conserver un document dont on ne pourrait garantir l'authenticité ?

4. Les bonnes raisons d'externaliser l'archivage électronique de vos documents

La mise en oeuvre d'un Système d'Archivage Electronique (SAE) répond donc à l'ensemble des besoins de l'entreprise en matière d'archivage numérique.

C'est un projet complexe et coûteux, qu'il est préférable d'externaliser.



4.1 POURQUOI LE SYSTEME D'ARCHIVAGE ELECTRONIQUE EST LA SEULE SOLUTION POUR MAÎTRISER L'ENSEMBLE DE VOS RISQUES

Vos collaborateurs n'ont pas toujours conscience que les documents électroniques qu'ils manipulent doivent être considérés comme des archives, et par conséquent ils ne pensent pas à les ranger correctement. Ces documents sont alors stockés de façon désordonnée dans les filesystem : arborescences Windows, disques durs, réseau de l'entreprise. Potentiellement accessibles par n'importe qui et de n'importe où, ces documents génèrent des risques multiples pour l'entreprise : financiers, juridiques, patrimoniaux...

La survenue effective d'un risque provoque souvent une prise de conscience au sein de l'entreprise et incite celle-ci à mettre en œuvre une solution d'archivage numérique.

Pour autant, une entreprise doit-elle développer elle-même son système ? Disposer en interne de sa propre infrastructure constitue un projet chronophage, coûteux à court, moyen et long terme, éloigné de son cœur de métier et risqué pour ses équipes. Autant de motifs pour envisager son externalisation auprès d'un tiers archiveur proposant des services mutualisés entre plusieurs entreprises.

4.2 LES 4 BONNES RAISONS D'EXTERNALISER VOTRE SYSTEME D'ARCHIVAGE ELECTRONIQUE

4.2.1 Disposer d'une solution opérationnelle plus rapidement

Le SAE est une solution très complète en termes de fonctionnalités, et donc très complexe à mettre en oeuvre. La développer en interne exige du temps. Il faut évaluer les besoins, concevoir la solution, la développer, la tester, la déployer, la déboguer... au risque de se lancer dans une "usine à gaz" qui une fois opérationnelle ne correspondra plus aux besoins de l'entreprise, qui auront évolués entre temps.

Au contraire, faire appel à un prestataire extérieur qui dispose d'une solution déjà éprouvée permet de disposer d'un service déjà opérationnel. Ce dernier pourra immédiatement être intégré à votre stratégie et mis au service de ses objectifs.

4.2.2 Maîtriser vos coûts d'archivage

Construire votre propre SAE coûte cher, le maintenir dans des conditions opérationnelles également. Les exigences auxquelles doit répondre un SAE impliquent de recourir à de multiples expertises et requièrent un matériel performant et récent, qui devra être renouvelé au gré des maintenances et des migrations.

A l'inverse, la mutualisation permet d'économiser des ressources et de partager tous les coûts du service : hommes, machines et logiciels... L'entreprise gagne également en visibilité financière : une seule ligne budgétaire couvre l'ensemble des dépenses, qui dans une solution interne seraient réparties sur différents postes (salaires, formations, investissements, amortissements...).

La mutualisation permet enfin de bénéficier d'un prix proportionnel à son activité, puisque la facturation est le plus souvent fonction du volume ou du nombre de documents archivés.

4.2.3 Se concentrer sur votre métier

Choisir de développer en interne votre SAE implique souvent pour votre DSI de changer de métier et d'acquérir de nouvelles compétences : il faut commander un audit à des consultants, recruter de nouvelles compétences, lancer des appels d'offre pour acquérir des technologies... avec des risques d'erreurs et de tâtonnements. Pour les Ressources Humaines la tâche peut aussi être compliquée car il faut gérer des personnes et des expertises qui ne font pas le même métier que le reste de l'entreprise.

Externaliser la gestion de votre SAE permet de rester concentré sur votre coeur de métier.

4.2.4 Se reposer sur l'expertise et les infrastructures d'un professionnel extérieur

La gestion d'un SAE constitue une grosse responsabilité pour votre DSI. En effet, pour les solutions numériques, le risque est proportionné à l'usage : les objets numériques ont l'avantage d'être faciles à créer, multiplier, transmettre... Ils répondent à vos besoins de rapidité et d'efficacité, mais sont en contrepartie plus fragiles car exposés aux dangers de divulgation et de corruption.

Le SAE constitue un enjeu de taille, la pression sur la DSI sera très importante, dans un contexte technologique très volatile qui nécessite une veille constante. Il paraît plus prudent de s'appuyer sur les infrastructures et l'expertise d'un prestataire spécialisé capable de fournir des prestations conformes à l'Etat de l'art et qui prendra en charge la maintenance, les migrations des supports et des formats...

LES ENGAGEMENTS DU TIERS ARCHIVEUR AU SERVICE DE LA PERENNITE NUMERIQUE

Obligation contractuelle de garantir la pérennité des supports de conservation

Le tiers archiveur doit disposer des expertises et des moyens technologiques pour éliminer le risque d'une perte ou d'une corruption de données. Cela implique de disposer d'une batterie de baies de stockage et du savoir-faire pour procéder à des migrations massives.

Engagement à permettre la réversibilité du Système d'Archivage Electronique

L'objectif est de migrer les archives d'un système d'archivage à un autre, sans perte de documents et en conservant la traçabilité des transactions réalisées. Toutes les opérations de conversion (dans un autre format) et de migration (vers un autre serveur) doivent être notifiées dans les journaux afin de garantir l'intégrité des archives.

Devoir de conseil sur les formats

En se basant sur une analyse coût / risque, le tiers archiveur doit déclencher des alertes sur les formats générateurs de risques et identifier les solutions les plus pertinentes au regard des archives à préserver.

En cas de conservation à très long terme de documents textuels, il peut par exemple préconiser une rematérialisation des archives électroniques. Celles-ci seront imprimées sur papier ou gravées sur microfilms. S'il s'agit de conserver ces documents pendant 80 ans, le choix de cette solution permet de diviser le coût d'archivage par 100.

EN CONCLUSION : développer votre propre système d'archivage en interne nécessite des investissements importants à long terme : infrastructures informatiques et logicielles, moyens humains, procédures, certifications...

Votre entreprise devra être en mesure de démontrer la conformité d'un consentement signé électroniquement aujourd'hui, et ce dans 20 ou 30 ans. Un certificat numérique doit être renouvelé tous les 2 ou 3 ans. Quant au dispositif technique qui permet de générer la signature, il doit être renouvelé tous les 5 à 10 ans.

Les moyens techniques seuls ne permettent pas de gérer tout le cycle de vie d'un document, ce qui est le rôle de l'archivage, qui permet de conserver à très long terme le document lui-même mais aussi sa signature et les preuves de validité du certificat au moment de la signature.

5. Les critères à prendre en compte pour choisir votre solution

| 7 CRITERES POUR FAIRE LE BON CHOIX | |
|------------------------------------|---|
| 1 | CONFIANCE ET CONFORMITE <ul style="list-style-type: none">• Certification NF Z 42-013• Label FNTC-TA (Tiers Archiveur) Selon votre activité, 2 autres agréments sont incontournables : <ul style="list-style-type: none">• Agrément Archives Publiques• Agrément « Hébergeur de Données de Santé » |
| 2 | SOLUTION MADE IN FRANCE <ul style="list-style-type: none">• Mise en œuvre par une société française• Données localisées sur le territoire français et soumises à la loi française |
| 3 | SOLIDITE ET PERENNITE DU PRESTATAIRE <ul style="list-style-type: none">• Stabilité financière• Indépendance |
| 4 | REDONDANCE DU SYSTEME <ul style="list-style-type: none">• Infrastructures et métadonnées• Sécurité renforcée et protection contre les risques de perte• Continuité de service en cas de défaillance |
| 5 | AUDITS REGULIERS <ul style="list-style-type: none">• Internes• Externes par un organisme certifié |
| 6 | REVERSIBILITE DU DISPOSITIF <ul style="list-style-type: none">• Récupération des données, documents et de la chaîne de traçabilité• Format interopérable FNTC |
| 7 | PRISE EN COMPTE DE L'ENSEMBLE DE VOS BESOINS <ul style="list-style-type: none">• Disponibilité, confidentialité, pérennité et intégrité des documents• Autonomie d'administration• Facilité d'utilisation• Prise en charge de l'ensemble de vos flux de documents• Connexion à vos systèmes d'information : outils métier (ERP, SIRH...), GED... |

LOCARCHIVES

VOUS ACCOMPAGNE DANS VOS PROJETS DE
DEMATERIALISATION ET D'ARCHIVAGE ELECTRONIQUE

Conseil et accompagnement

Numérisation

Transfert sécurisé des documents

Archivage Electronique et Physique

Gestion collaborative des documents et dossiers

01.49.33.78.81

contact@locarchives.fr

locarchives.fr

