ARCHIVAGE SUR LE CLOUD
PRATIQUES ET PERSPECTIVES

Publication Janvier 2014

Sommaire

PREFACE

Le passage du non connecté au tout connecté est une réalité technique et économique qui s'impose à tous. L'économie de service liée à la mutualisation des infrastructures et des logiciels sur Internet se développe pour permettre à chacun d'optimiser ses coûts et son temps tout en maitrisant ses risques.

A plusieurs reprises, les entreprises ont été amenées à faire des choix sur leur politique d'externalisation de leurs infrastructures et de leurs données. Certaines sont passées de l'internalisation, à l'externalisation partielle ou totale de leur système d'information. Les entreprises âgées, se sont développées sans Internet et ont dû s'adapter pour rester compétitives en utilisant, dans un premier temps Internet comme moyen de communication et d'information. Les entreprises plus récentes se sont développées avec l'arrivée d'Internet permettant de donner de nouvelles activités et de nouveaux modes de communication et d'échange. Tous ces changements rapides ont donné lieu à une structuration des échanges et des services au travers des normes et règlements sectoriels.

Les entreprises de demain utiliseront et se développeront nativement avec le Cloud. Cette évolution est inéluctable car elle est source d'économie et de compétitivité. L'offre est déjà fortement présente et les services fleurissent pour permettre de mettre en œuvre une économie numérique basée sur l'usage du Cloud.

Les documents et les données des entreprises sont au cœur du système d'information et seront demain sur le Cloud. Ces informations représentent le patrimoine économique et stratégique des entreprises. L'archivage numérique, encore très internalisé ou externalisé d'une manière confidentielle, devra pouvoir s'intégrer dans cette nouvelle économie.

Fort de son expérience autour des travaux normatifs et réglementaires liés à l'archivage numérique, l'APROGED, acteur majeur du développement économique des technologies de l'information, a souhaité publier ce livre blanc pour permettre de développer les axes de réflexion qui donneront lieu à des évolutions indispensables du cadre normatif et règlementaire.

Christian DUBOURG
Secrétaire APROGED

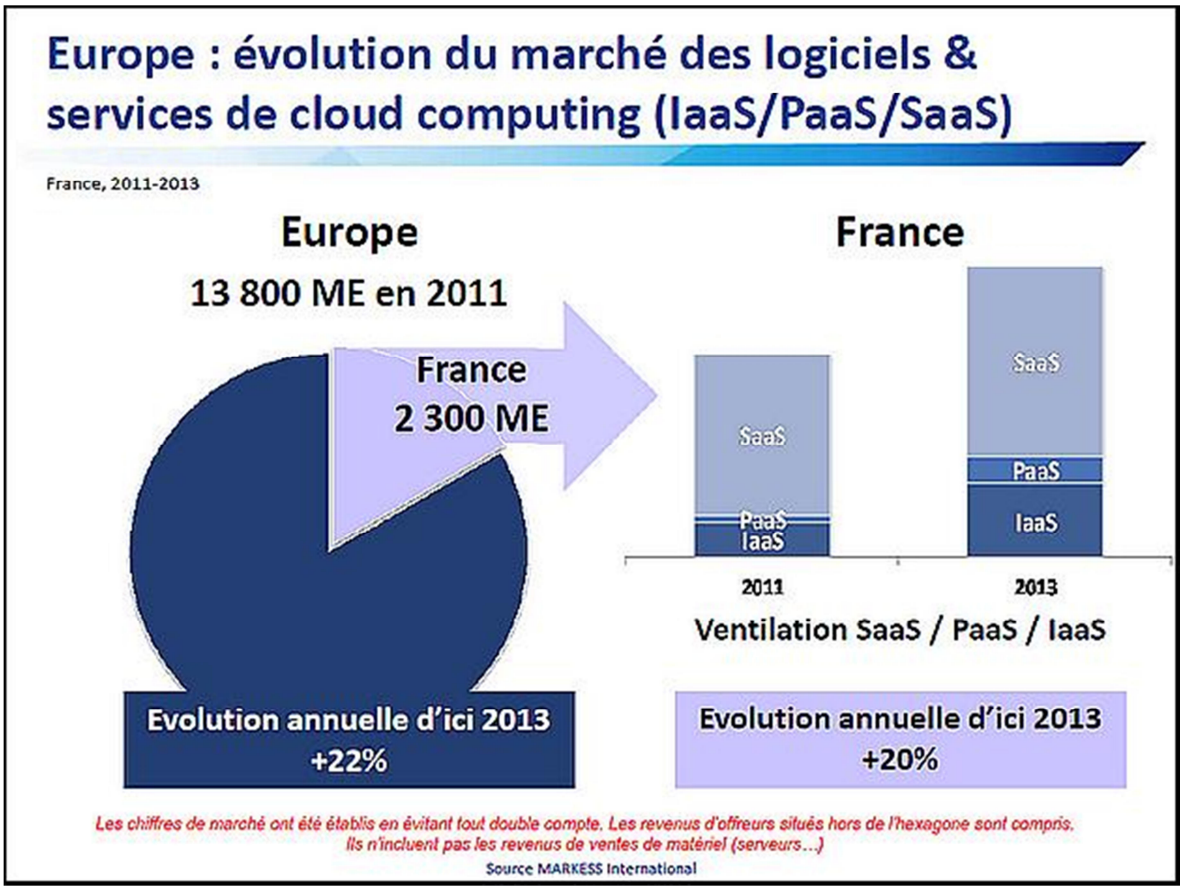
I. Etat de l'Art du Cloud pour l'archivage numérique

Les offres d'archivage sur le Cloud

1. Archivage sur le cloud : approches IaaS et SaaS

Selon IDC France dans son communiqué de presse de Mars 2013, les ventes de solutions Cloud Computing en mode SaaS en France ont représenté 7 % du marché logiciels en 2012, et ont bénéficié d'une croissance annuelle supérieure à 30%.

L'étude du cabinet français MARKESS International intitulée « Attentes et potentiels pour les infrastructures (IaaS) et les plateformes (PaaS) 2011-2013 » indique une croissance annuelle de 20% du marché du Cloud Computing en France, et précise que le mode SaaS constitue l'essentiel du marché du Cloud Computing sans nuire à la croissance des modes IaaS et PaaS.



Source MARKESS international

L'archivage électronique est une des fonctions support des entreprises contribuant à la croissance du marché du Cloud Computing.

1.1. L'approche IaaS de l'archivage sur le cloud :

L'infrastructure en tant que service IaaS (Infrastructure as a Service) est un modèle de Cloud Computing dans lequel :

- Un prestataire fournit l'infrastructure :
  - Le ou les serveurs.
  - Les couches de virtualisation.
  - Le stockage.
  - Les réseaux.
- L'entreprise utilisatrice gère :
  - Le système d'exploitation des serveurs.
  - Les logiciels applicatifs dont celui du Système d'Archivage Electronique.

L'entreprise utilisatrice fait donc l'acquisition des licences pour le Système d'Archivage Electronique et prend à sa charge la mise en œuvre de ce logiciel. L'entreprise utilisatrice loue auprès du prestataire une infrastructure Cloud comprenant des serveurs, du stockage et du réseau avec un modèle de paiement en fonction de l'utilisation.

L'entreprise utilisatrice accède à cette infrastructure sur Internet pour mettre en œuvre et gérer son Système d'Archivage Electronique :

Gestion des ressources IaaS par l'entreprise utilisatrice

Les offres IaaS reposent sur des techniques de virtualisation. L'entreprise utilisatrice construit son infrastructure d'archivage électronique et la fait évoluer selon ses besoins : ressources CPU, mémoire, espaces de stockage, bande passante réseau, firewall dédié, gestion des comptes utilisateurs.

Délégation de la sécurité IaaS auprès du prestataire

Le prestataire IaaS prend en charge l'hébergement et la sécurité physique du matériel lié aux supports d'archivage et aux serveurs : redondance des équipements, sécurité 24/24 et 7/7, surveillance vidéo, climatisation, détection incendie. La sécurité applicative est assurée par des services d'authentification mis en place par le prestataire. L'exploitation est réalisée par le prestataire.

Mise en place d'un réseau sécurisé

Dans la majorité des cas, pour accéder aux serveurs en mode IaaS, un VPN (Virtual Private Network) permet de relier l'entreprise utilisatrice avec le prestataire. La garantie de qualité de service et de sécurité des réseaux est du ressort de prestataires de télécommunications.

1.2. L'approche SaaS de l'archivage sur le cloud :

La solution logicielle en tant que service SaaS (Software as a Service) est un modèle de Cloud Computing dans lequel :

- Un prestataire fournit à la fois l'infrastructure et la solution d'archivage :
  - Le ou les serveurs.
  - les couches de virtualisation.
  - le stockage.
  - les réseaux.
  - le système d'exploitation des serveurs.
  - les logiciels applicatifs dont celui du Système d'Archivage Electronique.
- L'entreprise utilisatrice loue auprès du prestataire un service tarifé notamment selon :
  - Des licences pour le Système d'Archivage Electronique sur la base d'un loyer mensuel incluant la maintenance logicielle.
  - Une infrastructure Cloud nécessaire : serveurs, stockage et réseau avec un modèle de paiement en fonction de l'utilisation.
  - Les autres types de services spécifiés contractuellement.

L'entreprise utilisatrice consomme alors la solution d'Archivage Electronique à la demande, en fonction de ses besoins réels.

Gestion des ressources SaaS par le prestataire

Les offres SaaS reposent aussi sur des techniques de virtualisation. Le prestataire gère l'infrastructure d'archivage électronique et la fait évoluer selon les besoins de l'entreprise utilisatrice : ressources CPU, mémoire, espaces de stockage, bande passante réseau, firewall dédié, gestion des comptes utilisateurs.

Délégation de la sécurité SaaS auprès du prestataire

En plus des garanties offertes par le fournisseur IaaS, le prestataire SaaS prend en charge la sécurité du système d'archivage électronique. La sécurité applicative est assurée par des services d'authentification mis en place par le prestataire. L'exploitation de la solution est réalisée par le prestataire.

Mise en place d'une communication sécurisée

Pour accéder à sa solution d'Archivage Electronique en mode SaaS, une communication sécurisée entre le client et son prestataire est mise en place. Des protocoles de communication sécurisés (ftps, https, ...) sont mis en œuvre pour les différentes fonctions du SAE (versement, communication, ...).

2. Modes d'archivage hybrides

Traditionnellement les systèmes d'archivage sont mis en œuvre en interne. Sur la base des différents services possibles (SaaS, PaaS, IaaS), plusieurs architectures peuvent se décliner mixant approche interne et cloud, jusqu'à une externalisation complète.

Un système d'archivage peut, de façon très synthétique, être découpé en trois sous-ensembles :

- La politique d'archivage et les fonctions de référencement.
- Des fonctions contribuant à la valeur probatoire.
- Les fonctions de stockage.

C'est dans la répartition de ces ensembles que les solutions intermédiaires interne / Cloud pourront varier. Les motivations des entreprises sont principalement de l'ordre de l'optimisation financière tout en conservant en interne la maitrise de certains composants jugés critiques ou à risques.

Les fonctions de stockage :

Dans les systèmes d'archivage, les fichiers sont en général stockés au moins en deux exemplaires afin d'offrir des garanties de pérennité. Le stockage des fichiers dans le Cloud peut porter sur l'ensemble de ces instances ou seulement une partie d'entre elles, les autres restants alors stockées en interne.

Dans ce type de configuration, il sera nécessaire d'être extrêmement vigilant sur les acquittements touchant aux opérations sur les fichiers (attestations de versement et de destruction et autres mouvements)

Les fonctions contribuant à la vocation probatoire

Les fonctions contribuant à la vocation probatoire peuvent être portées :

- Par le logiciel d'archivage.
- Par l'infrastructure de stockage sécurisée.
- Par une combinaison logiciel/infrastructure.

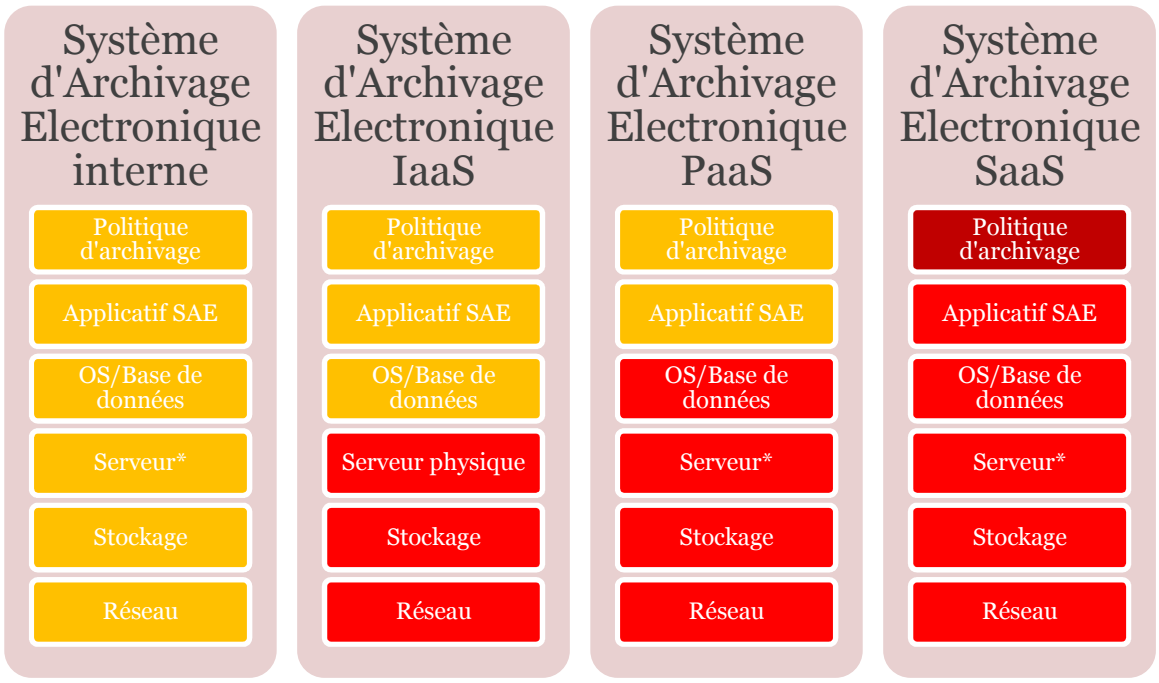
En cas de portage même partiel des fonctions contribuant à la vocation probatoire par l'infrastructure mise à disposition dans le Cloud, il sera nécessaire, outre les éléments définis dans les fonctions de stockage de prendre en compte ceux liés à la traçabilité tout particulièrement s'ils restent stockés au niveau de l'infrastructure Cloud.

Au-delà de ces répartitions des ensembles fonctionnels, il faut également considérer que la configuration du système d'archivage peut être modulée en fonction des types de documents ainsi que des contraintes et risques qui y sont associés dans la mesure où les systèmes d'archivage peuvent piloter la stratégie de stockage en fonction de règles.

Ainsi une solution d'archivage hébergée en interne et disposant également d'espaces de stockage internes et externes dans le Cloud peut **par exemple** orienter :

- vers les espaces de stockage internes certains types de données comme les données à caractères personnels ou les documents confidentiels,
- à la fois vers les espaces internes et les espaces externes (une instance de chaque côté) pour les types de données nécessitant une consultation ou une remise en ligne rapide,
- vers les espaces de stockage externes pour les autres types de données.

Il existe de multiples configurations d'implémentation du système d'archivage mixant approche interne et Cloud permettant de moduler le système à ses besoins. Cependant il faut prendre en compte les impacts notamment sur les clauses contractuelles avec le fournisseur Cloud et sur une éventuelle certification dont il faut garder en mémoire qu'elle peut elle aussi être ciblée.



* Le serveur peut être physique ou virtuel

L'entreprise a le contrôle
L'entreprise partage le contrôle avec le fournisseur de service
Le fournisseur de service a le contrôle

- **IaaS** – infrastructure à la charge du fournisseur
- **PaaS** – infrastructure et prérequis à la charge du fournisseur
- **SaaS** – service d'archivage à la charge du fournisseur, PA partagé (préparation des flux, gestion des habilitations… à la charge du client)

3. Archivage sur le Cloud : approche Cloud public (mutualisé pour plusieurs clients) et Cloud privé (dédié à un client)

On note ici la majuscule du mot « Cloud », même si le nuage est loin de s'unifier. Une offre de service cloud a vocation à bénéficier d'une économie d'échelle, et donc à mutualiser tout ou partie des « couches ». Dans ce contexte, le cloud privé est une allocation particulière de ces ressources, et trouve donc une limite dans la mutualisation. En revanche il offre une continuité plus naturelle avec les ressources internes et préexistantes de l'entreprise, et facilite le modèle « hybride » qui permet des transitions réalistes.

Pour ce qui concerne l'archivage dans le Cloud, il est en fait une possibilité d'archivage dans un ou plusieurs « clouds » publics. Pour simplifier prenons l'exemple d'un seul. La question de la mutualisation est alors une problématique à deux perspectives :

- **Celle du fournisseur** : la mutualisation peut concerner tout ou partie des couches, depuis l'infrastructure de calcul et de stockage jusqu'au logiciel d'archivage qui délivre selon les attributs attendus pour un archivage de qualité, ce mot pouvant avoir des degrés ; elle est essentiellement un arbitrage économique, en face de complexités plus ou moins faciles à gérer et de garanties à donner au client. La question se pose en particulier de la mutualisation des archives des différents clients. Or la crédibilité s'établit dans la durée, et se perd très vite en cas de problème.

- **Celle du client (la personne morale)** : la mutualisation des données est généralement perçue comme un risque. La vérification du niveau de service rendu est plus difficile, et il faudrait un avantage prix important pour que cette perception de risque soit acceptable. La réversibilité en serait également un critère, de même que la localisation des archives dont il est question plus bas et qui a plusieurs conséquences.

Dans la pratique, on se préoccuperait peu de la mutualisation d'un service de stockage de fichiers ouvert à tous sur le cloud. Cependant, on se préoccuperait de la mutualisation des données pour un archivage assurant la conformité de l'entreprise dans tous ses aspects réglementaires, y compris la localisation de ses archives. Les lecteurs ayant pratiqué une mutualisation totale, en tant que client ou en tant que fournisseur pourront apporter leur commentaire.

Au-delà de la mutualisation se pose finalement le problème de la responsabilité du fournisseur du service par rapport aux données de son client. Même s'il se dégage de cette responsabilité, il se peut que des réglementations sectorielles ou spécifiques à des pays évoluent et engagent la responsabilité du fournisseur comme du client. C'est déjà le cas dans le domaine de la santé (par exemple HIPAA aux Etats-Unis pour les aspects de protection des données personnelles, qui s'appliquent aux archives).

Localisation géographique des archives

La question de la localisation des archives est à traiter sous deux aspects.

1. **Origine géographique des données à archiver**

En premier lieu, comme les réglementations ne sont pas harmonisées à travers le monde et même au niveau européen, il faut considérer **l'origine géographique des données à archiver** afin de définir si les réglementations applicables compte tenu de cette origine définissent des conditions particulières d'archivage.

Ces restrictions sont généralement sectorielles. A titre d'exemple, on peut citer :

- L'International Traffic in Arms Regulation (ITAR) aux USA qui interdit l'exportation de toutes données techniques pouvant servir à des fins militaires.
- Les réglementations Suisse et Luxembourgeoise sur les données bancaires.
- Bien d'autres réglementations propres à l'Europe.

La réglementation française apporte également son lot de contraintes sur la conservation et l'éventuelle exportation des données :

Le transfert des données personnelles

Le transfert des données personnelles hors de l'Union européenne requiert [1] :

- La conclusion d'un contrat de transfert conforme aux clauses contractuelles type de la Commission européenne ou la mise en place de règles internes d'entreprise (Binding Corporate Rules).
- Une autorisation préalable de la CNIL sauf lorsque le transfert est à destination:
  - de pays reconnus par la Commission européenne comme satisfaisant à un niveau suffisant de protection des données,
  - d'entité aux Etats-Unis ayant par ailleurs adhéré aux principes du Safe Harbor.

L'hébergement des données de santé à caractère personnel

L'hébergement des données de santé à caractère personnel sur support informatique est strictement encadré[2] et est soumis à l'obtention d'un agrément national délivré en contrepartie de garanties en termes d'intégrité, de sécurité et de confidentialité. Le dossier d'agrément HADS précise notamment le lieu d'hébergement des données, toute modification devant être notifiée auprès du ministère de la Santé.

[1] La loi Informatique et Libertés du 6 janvier 1978 modifiée (transposition de la Directive européenne 95/46/CE) et le décret du 20 octobre 2005 modifié pris pour l'application de la loi n°78-17 relative à l'informatique et aux libertés

[2] Code de la Santé Publique – Article R.111-9 et suivants

Les secteurs bancaires et assurances

Les secteurs bancaires et assurances sont soumis[3] à des obligations de contrôles et de formalités supplémentaires.

La conformité réglementaire

La conformité par rapport au droit doit être respectée. Il y a en particulier obligation légale de ne pas entraver l'exercice de la justice qui peut exiger d'accéder à certaines données ce qui peut s'avérer compliqué voire impossible en dehors de l'Union européenne.

L'auditabilité des lieux d'archivage

La Marque NF 461 qui s'applique aux systèmes d'Archivages Numériques précise dans ses règles de certification : « **Est exclu de la certification, tout demandeur dont le SAE ne permet pas de connaître et de maîtriser la localisation et l'élimination des documents numériques ».**

Il faut entendre par « localisation » le lieu géographique dans lequel se trouvent archivées les contenus numériques.

Dans le cadre de l'audit de certification du SAE, un examen documentaire vérifie les conditions physiques décrivant la localisation des sites géographiques.

L'auditeur vérifie l'existence d'au moins deux sites d'archivage et réalise une visite de chaque site afin de vérifier l'application des modalités décrites dans le « Dossier de Description Technique du Système ».

Des réflexions sont en cours pour définir une norme autour des objets numériques et de leurs propriétés dont la localisation.

2. Législations des pays où sont hébergées les données.

En second lieu, il faut considérer les législations des pays où sont hébergées les données car les lois de protection des données varient elles aussi en fonction des pays.

Lors d'un colloque organisé par la CNIL[4] et l'université Panthéon-Assas-Paris II au Sénat les 7 et 8 novembre 2005, M. Robert Gellman, avocat auprès de la Cour suprême de Pennsylvanie et expert-conseil en protection des données, soulignait que la méthode américaine de régulation de la protection des données personnelles était éloignée de l'approche européenne, qui repose sur **des normes complètes de protection** et sur **l'existence d'une autorité indépendante de protection des données.**

[3] Code des Assurances - R. 336-1f, Code de la Mutualité 211-28f , Code de la Sécurité Sociale - R. 931-43f, Règlement CRBF n°97-02)

[4] http://www.senat.fr/colloques/colloque_cnil_senat/colloque_cnil_senat_mono.html
http://www.senat.fr/rap/r08-441/r08-44128.html

Les Etats-Unis ne disposent pas d'une autorité indépendante dédiée à la protection des données et n'ont pas de cadre général de protection des données dans le secteur privé mais des lois sectorielles. La régulation du marché est privilégiée à l'intervention de l'Etat. Cette régulation est soit volontaire par l'élaboration de codes de bonne conduite internes à l'entreprise, soit contractuelle par le biais de conventions entre les opérateurs économiques et les consommateurs.

Certains pays sont dotés d'une législation très stricte avec des lois anti-terroristes, d'espionnage industriel ou de façon plus générale de règles d'ordre public qui permettent aux autorités publiques nationales de contraindre des prestataires de Cloud à communiquer les informations de leurs clients qu'ils détiennent sur le territoire de ces pays. C'est le cas par exemple des Etats-Unis avec le Patriot Act et le Foreign Intelligence Surveillance Act.

La localisation des données est un point essentiel qui doit être traité et vérifié par l'entreprise afin de s'assurer que toutes les contraintes réglementaires ont été anticipées tant sous l'angle des réglementations (localisation, auditabilité, protection, ...) à respecter du fait de l'origine des données que celles applicables du fait de leur localisation d'hébergement (confidentialité, divulgation, ...).

Contraintes et responsabilités

1. Identification des données à archiver.

Au même titre que pour la localisation géographique des archives, les réglementations et contraintes qui s'appliquent peuvent varier **en fonction du secteur d'activité** voire du type de données. Les cas de réglementation sectorielle sont nombreux comme par exemple dans les domaines suivants :

- Assurance (Solvency II, Code des Assurances, ...)
- Bancaire (Bâle II et III, MiFID, ...)
- Finance (Sarbanes-Oxley Act, AMF, ...)
- Pharmaceutique (ISPE GAMP, CFR 21 Part 11, ...)
- Chimie (REACH, ...)
- Santé (Code de la Sécurité Sociale, Code de la Santé Publique, ...)
- ...

Ces réglementations peuvent être aussi bien **nationales** que **multinationales** (Directive européenne, Autorités de tutelles régionales, ...).
Il existe également des réglementations propres à certains types de données comme par exemple :

- Les données à caractère personnel (CNIL)
- Les factures (directive européenne du 13/07/2010 et transposition par les décrets du 24 et 25/04/2013, Code du commerce, ...)
- Les bulletins de paye (Code du travail, loi de simplification des procédures, ...)
- ...

Outre ces réglementations "externes" qui peuvent générer des contraintes particulières, il faut également que les entreprises examinent leurs **réglementations "internes"** (procédures, plans qualité, plans de sécurité, ...), lorsqu'elles existent et sont formalisées, complétées le cas échéant par un positionnement par rapport aux enjeux et risques. Ce positionnement permettra de faire émerger d'autres données qui seront considérées comme stratégiques (recherches en cours, procédés de fabrication, ...) ou sensibles (financières, données concurrentielles, ...).

La démarche d'analyse des risques intégrant une analyse de la valeur permet à chaque entreprise d'adapter à son contexte sa politique d'archivage en prenant en considération la dimension économique (coût de possession versus peine/coût si le risque intervient). **L'approche "cloud" est l'une des composantes significatives permettant d'agir sur le coût de possession des archives**.

Cette analyse doit également prendre en compte le paramètre temps :

- La probabilité de devoir restituer certaines données peut varier pendant leur durée de conversation.
- Le caractère de sensibilité de certains documents peut lui aussi évoluer.

De ce fait, il est également envisageable pour un même type de données de s'orienter vers une approche alternant archivage interne et archivage cloud en fonction du positionnement dans le temps.

2. Impact du Cloud sur le cycle de vie des données à archiver

Archiver dans le « nuage » ne change pas la nature de l'archive. L'archive est un état particulier d'un document à un moment de son cycle de vie qui va de sa création à son sort final (destruction, versement aux archives nationales etc.).

Gouverner le cycle de vie d'un document, c'est lui appliquer des politiques conformes à la réglementation d'un pays donné, et souhaitées par l'entreprise. Ces politiques peuvent concerner la durée de conservation, et d'autres paramètres comme la confidentialité dont le degré pourra éventuellement diminuer dans le temps, ou la protection des données personnelles qui pourra évoluer vers l'anonymisation.

Il n'y a pas à proprement parler de différence entre les politiques applicables à des archives dans le nuage et celles applicables à des archives restées dans l'entreprise. Par exemple, dans les deux cas, la destruction « opposable » d'archives répond à un objectif de réduction de coût et de risques.

Or nous avons vu que le modèle hybride où coexistent des archives dans l'entreprise et des archives dans le nuage est le plus vraisemblable, au moins pour des organisations d'une certaine importance.

Il est donc souhaitable d'harmoniser les politiques et les moyens d'en forcer l'application où que soient gérées les archives. C'est le rôle d'une plateforme de gouvernance de l'information, capable d'inclure le cloud.

Il est également intéressant de noter que si cette harmonisation est effective, elle facilite la migration de contenu et en particulier d'archives vers le cloud.

D'autant mieux que les politiques de gouvernance couvrent un des aspects les plus sensibles du cloud : la protection des données personnelles, et leur transfert vers des pays aux réglementations problématiques.

3. Les archives publiques en France et les contraintes associées à l'archivage dans le Cloud.

Un corpus de lois et décrets définit, depuis 1979, les règles de gestion des **archives publiques** et de protection des archives privées, qui s'appliquent à tous les organismes publics, nationaux ou locaux. La dématérialisation, et la conséquente facilité à externaliser les archives, ont provoqué d'une part un changement majeur dans le métier des archivistes et de l'autre ont induit une évolution de celui des fournisseurs des services. Conjuguer la performance et la rigueur est une nécessité aussi bien pour le secteur privé et le service public. C'est l'enjeu du fournisseur d'un service d'archivage dans le Cloud.

Le Code du patrimoine définit les trois âges des archives, constituant le cycle de vie des documents (art. R.212-10, R.212-11 et R.212-12)

Le service d'archivage Cloud doit être dédié à la conservation à vocation probatoire de fonds d'archives électroniques courantes et intermédiaires, pour les besoins de la sphère publique, au plan national comme aux échelons territoriaux. Ce service doit offrir une solution assurant la gestion complète des 4 C de l'archivistique (collecte, classement, conservation et communication) et peut y ajouter les bénéfices économiques de la mutualisation.

Une approche basée sur les procédures constitutives du système de management des archives (SMA) :

- Versements conformes au SEDA, structurés par DTD ou l'application métier ou saisis en mode interactif,
- Gestion du cycle de vie des archives en entrée,
- Consultation et communication des documents archivés dans le strict respect des règles de communicabilité,
- Collecte des archives par transferts,
- Destruction des archives éliminables à DUA échue et dans le strict respect du CST de l'Etat,
- Restitution partielle ou totale des archives déposées dans le SAE,
- Conformité à la NF Z42-013:2009,
- Niveau de sécurisation standard, constituant un élément supplémentaire de l'appréciation en terme d'intégrité, de pérennité, de sécurité et de traçabilité afin de diminuer le risque de remise en cause du système.

Justificatifs des opérations d'archivage

- Transferts d'archives
- Communication d'archives
- Elimination d'archives
- Restitution d'archives

Procédure de transfert d'archives

- Edition du bordereau
- Soumission de la demande
- Traitement pour validation
- Import dans le SAE
- Journalisation et contrôle

Procédure de consultation ou de communication d'archives

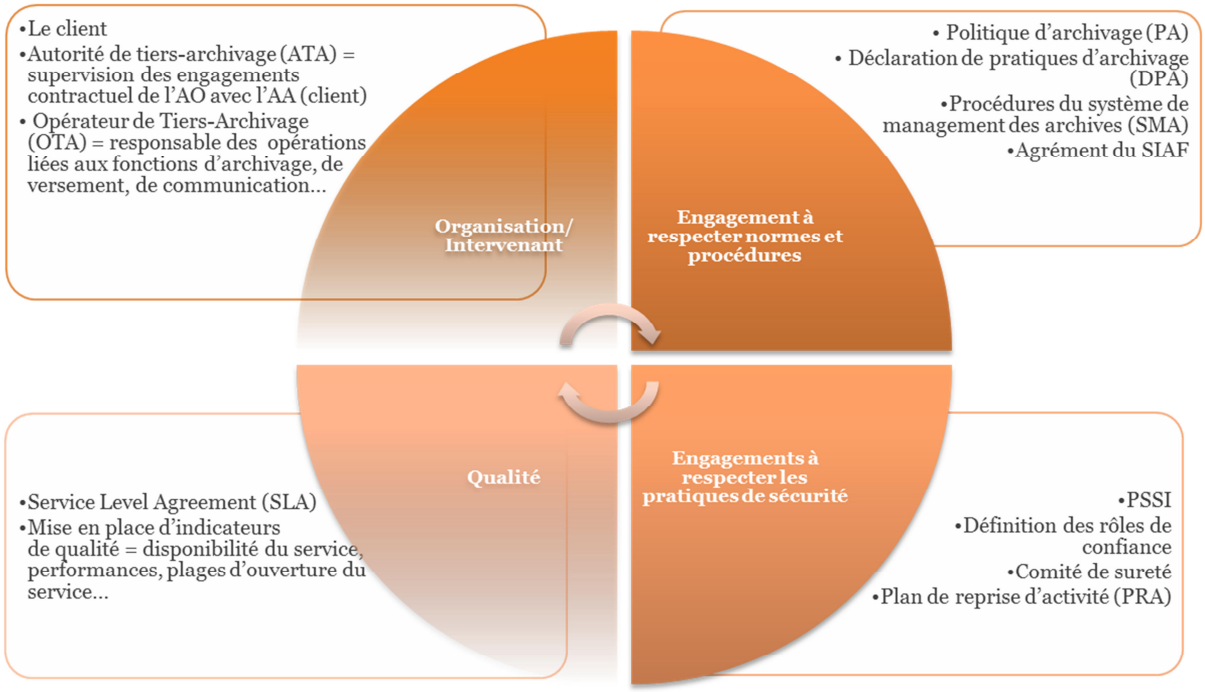
- Vérification des prérequis
- Recherches multicritères sur les métadonnées
- Consultation d'archives
- Communication d'archives à un service demandeur
- Journalisation et contrôle

Procédure d'élimination d'archives

- Vérification des prérequis (ex. DUA)
- Types d'éliminations (unitaires, par lots)
- Génération du bordereau d'élimination
- Validations
- Destruction
- Journalisation et contrôle

Procédure de Restitution d'archives partielle ou totale

- Validation des prérequis
- Demande de restitution et validation
- Restitution des archives
- Acquittement de la restitution
- Elimination des archives restituées
- Journalisation et contrôle


•Le client
•Autorité de tiers-archivage (ATA) = supervision des engagements contractuel de l'AO avec l'AA (client)
• Opérateur de Tiers-Archivage (OTA) = responsable des opérations liées aux fonctions d'archivage, de versement, de communication…
Organisation/ Intervenant
• Politique d'archivage (PA)
• Déclaration de pratiques d'archivage (DPA)
•Procédures du système de management des archives (SMA)
•Agrément du SIAF
Engagement à respecter normes et procédures
•Service Level Agreement (SLA)
•Mise en place d'indicateurs de qualité = disponibilité du service, performances, plages d'ouverture du service…
Qualité
Engagements à respecter les pratiques de sécurité
•PSSI
•Définition des rôles de confiance
•Comité de sureté
•Plan de reprise d'activité (PRA)

4. Contrats du Cloud et contrats pour l'archivage

Dans le cadre d'une solution d'archivage externalisée, il appartient à l'utilisateur du service de vérifier le contrat qui l'unit à son ou ses fournisseurs de service. L'acception des clauses d'un contrat établit l'acte de reconnaissance des responsabilités de chacun.

Les contrats qui encadrent les services Cloud doivent être adaptés à **l'archivage sur le Cloud**. Ils doivent prendre en compte des clauses compatibles avec la politique d'archivage des clients potentiels.

La politique d'archivage du client

Avant de décider d'utiliser des services Cloud pour l'archivage des documents numériques, il est indispensable de vérifier la **présence d'une politique d'archivage** de l'entreprise utilisatrice du service Cloud. Comme le précise le livre blanc du CR2PA sur le sujet intitulé « Politique d'archivage, guide méthodologique », la politique d'archivage est un élément de la politique de gouvernance et permet de traiter des trois enjeux majeurs et stratégiques liés à l'archivage des contenus de l'entreprise :

- Répondre aux exigences légales et réglementaires en termes de conservation des documents,
- Protéger les savoirs et savoir-faire,
- Limiter la mise en cause de la responsabilité de la société et de ses dirigeants.

Ces enjeux doivent être complétés par une **analyse des risques** permettant d'identifier pour chaque type de risque, les impacts financiers, juridiques et opérationnels.

4.1.La politique d'archivage

- **En SaaS**

Dès lors qu'un fournisseur de services propose un service d'archivage sur le Cloud en mode SaaS, il doit lui-même mettre en place sa politique d'archivage permettant de définir les enjeux et les risques associés aux documents numériques qui lui sont confiés par ses clients. Cette politique d'archivage ne peut pas être adaptée à chaque type de client car le modèle économique du Cloud n'est pas toujours adapté à une personnalisation contractuelle. Il est indispensable de vérifier que la politique d'archivage de l'entreprise faisant appel au service Cloud est compatible avec la politique d'archivage proposée contractuellement par le fournisseur de service.

- **en IaaS**

La politique d'archivage qui s'applique est celle de l'utilisateur du service. Il a une totale liberté dans la mise en oeuvre de sa politique d'archivage.

4.2. Le contexte de l'Europe

Suite à l'affaire Prism, la Commission européenne a décidé de mettre en place un groupe d'experts pour travailler sur la **définition des clauses contractuelles types** d'un contrat de services pour l'utilisation du Cloud en Europe. Les futurs contrats de service pour les entreprises présentes sur le territoire européen tiendront compte du fruit du travail de la Commission européenne.

4.3. Le contexte de la France

La CNIL a publié dans un document récent, des « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing ». Même si ce document n'est pas exclusivement lié à l'archivage dans le cloud, il doit être étudié et pris en compte pour vérifier que les contrats proposés par les fournisseurs de service, contiennent des clauses qui couvrent les risques majeurs liés à l'utilisation du Cloud.

Ce document précise les sept recommandations suivantes :

- Identifier clairement les données et les traitements qui passeront dans le Cloud.
- Définir ses propres exigences de sécurité technique et juridique.
- Conduire une analyse de risques afin d'identifier les mesures de sécurité essentielles pour l'entreprise.
- Identifier le type de Cloud pertinent pour le traitement envisagé.
- Choisir un prestataire présentant des garanties suffisantes.
- Revoir la politique de sécurité interne.
- Surveiller les évolutions dans le temps.

Tiers Archiveurs et archivage Cloud

Dans le domaine des documents numériques, le terme « Tiers Archiveur » tel que cité dans la norme NF Z42-013, désigne « la personne physique ou morale qui se charge pour le compte du Client d'assurer et de garantir la conservation de documents numériques ». L'externalisation du service est destinée à prendre en charge des contraintes opérationnelles, techniques, réglementaires et sécuritaires liées à l'exploitation de solutions et de plateformes.

L' « archivage Cloud » n'est que la projection du même service sur une infrastructure 'Cloud'. Bien que le service soit le même, il serait erroné de penser que le métier de Tiers Archiveur reste inchangé.

Le Tiers Archiveur 'Cloud' propose un service à **architecture variable**, c'est-à-dire que les ressources mises à disposition du client pour le versement, la recherche et la consultation des archives sont fonction de son besoin. C'est bien cette approche qui assure une proportionnalité entre la consommation du client et le prix payé pour le service : le bien connu mode SaaS.

Or une infrastructure distribuée, dont les frontières ne sont –par définition- pas maitrisées, ne correspond pas au besoin de tous les clients. L'offre de services proposée doit se conjuguer en fonction des exigences et contraintes légales et métier du client.
Le partage des ressources, et donc la garantie du niveau de service, ainsi que la localisation des supports de stockage sont deux points auxquels les fournisseurs doivent se confronter.

Un 'Cloud 100% français' s'impose pour la gestion des données de santé et pour les archives du service public. On parle souvent aussi de 'Cloud privé', pour désigner les infrastructures dédiées à un seul client ou verticales, pour les acteurs d'un métier très réglementée.

Le Tiers Archiveur qui passe à l'offre Cloud est en mesure de proposer des offres plus attractives tout en étant plus souples. Cet objectif est atteint par la maitrise des coûts, notamment par le partage des ressources qui ne sont utilisées que ponctuellement par chaque client, et la capacité et la facilité de répliquer rapidement des machines virtuelles.

Par la même occasion, il convient de préciser qu'un fournisseur de services IaaS et PaaS, qui dispose des mêmes caractéristiques en matière d'architecture, n'est pas pour autant un Tiers Archiveur Cloud. La gestion de l'application (le SAE), la compétence métier, l'accompagnement du client et la capacité de conseil en phase projet sont les atouts d'un fournisseur de service SaaS, pas d'un fournisseur d'infrastructure ou de plateforme.

Editeurs de logiciel et archivage Cloud

Les éditeurs de logiciel d'archivage ne peuvent ignorer et n'ignorent pas le Cloud.

Les solutions d'archivage à venir devront offrir un volet cloud, et gérer la coexistence entre les deux contextes. Elles devront probablement gérer la migration de tout ou partie du contenu vers le cloud, au rythme choisi.

Mais les éditeurs de logiciel d'archivage ont aussi la possibilité de faire évoluer leur modèle, et devenir également des offreurs de services d'archivage SaaS.

On retrouve ici la discussion faite plus haut sur la mutualisation dans le nuage, et les responsabilités que l'offreur de service est amené à prendre. Le lien entre la solution SaaS et la vie des systèmes dans l'entreprise peut ressembler au mécanisme de versement/consultation décrit plus haut, mais le marché évolue actuellement vers une prise en charge holistique du cycle de vie de l'information. Ce qui multiplie les points de contact entre processus métier et conteneurs de l'information, le tout sous une couche de gouvernance.

Le Cloud qui facilite l'aggrégation de services engendrera probablement des approches nouvelles, voire disruptives.

Le Cloud Services Brokerage

Avec l'arrivée du « **Cloud Services Brokerage** », de nouvelles offres montées par des intégrateurs et des éditeurs de logiciels voient le jour. Le **CSB** (Cloud Service Brokerage) consite à mettre en œuvre un **portail d'accès** à un ou plusieurs services Cloud (privés ou publics) via de **l'agrégation** de services, de **l'intégration** et de la **personnalisation**.

Le Cloud Broker permet à ses clients d'offrir **des bouquets de services**, d'en maitriser l'usage et la facturation.

Le rôle d'intégration consiste à **véhiculer des données d'un service à un autre** via un bus de services afin de permettre la mise en place de **processus de traitement** entre les différents services assemblés.

Enfin, le Cloud Broker peut également offrir des **fonctions de support** sur les services clouds utilisés et assemblés.

Le Cloud broking permet d'apporter la souplesse d'utilisation et d'intégration de services Cloud lorsqu'elle fait défaut ou lorsque plusieurs services doivent être intégrés les uns avec les autres.

C'est sans doute un passage obligé pour l'archivage des contenus numériques sur le Cloud lorsqu'une entreprise souhaite travailler avec plusieurs fournisseurs de services d'archivage sur le Cloud.

II. Sécurité et confidentialité sur le Cloud

Analyse de risques

A l'échelon européen, le groupe de travail «Article 29» institué par la directive 95/46/CE du Parlement européen sur la protection des données, a publié des recommandations relatives à l'égard du traitement des données à **caractère personnel** et à la libre circulation de ces données.

En France, la CNIL (Commission Nationale Informatique et Libertés) a publié le 25 Juin 2013 des recommandations à l'adresse des entreprises ou organisations confiant leurs données à des prestataires opérateurs sur le Cloud. Ces recommandations indiquent les clauses essentielles des contrats de prestations d'archivage sur le Cloud.
Ces clauses doivent être rédigées après une analyse des risques techniques et juridiques.

Chaîne de sous-traitants

La CNIL et le groupe de travail «Article 29» indiquent que **le client est le responsable du traitement** dans la mesure où il est à l'origine de la collecte des données et de la décision d'externalisation du traitement auprès du prestataire.

- Dans le cadre du Cloud privé, les services exclusivement sont dédiés à un client qui se doit de maîtriser et de déterminer les caractéristiques du service demandé au prestataire.
- Dans le cadre du Cloud public, les services font l'objet d'offres standard mutualisées auprès de plusieurs clients. Le client et le prestataire, son sous-traitant, sont dès lors conjointement responsables du traitement.

La chaîne de sous-traitance doit être maitrisée pour éviter la perte de contrôle et l'absence de transparence :

- La liste des sous-traitants et leur localisation géographique doit être fournie par le prestataire.
- Si le client accepte la sous-traitance, il doit être informé de toute nouvelle sous-traitance.

Durée de conservation des archives et des éléments de preuve

« Dans le cadre du Cloud, le prestataire doit s'engager à ne pas conserver les contenus archivés au-delà de la durée de conservation fixée contractuellement avec le client et à ne jamais conserver les contenus à la fin du contrat et après restitution. »

Panne du service et de son indisponibilité

Le SLA (Service Level Agreement) permet de garantir à un client d'une solution d'archivage sur le Cloud la disponibilité des données archivées et des services afférents (versements, consultations, restitutions).

Le prestataire doit assurer 3 principaux indicateurs

- Le niveau de disponibilité du réseau : le prestataire doit prévenir la rupture ou la saturation du réseau suite à la défaillance d'un des éléments de l'infrastructure réseau. Au-delà de l'infrastructure réseau du prestataire, le client doit lui-même surveiller la disponibilité de sa propre connectivité à Internet ou au réseau privé le reliant au prestataire.

- Le niveau de disponibilité des services de consultation : celui-ci est en général proposé par le prestataire à 99,9 % ce qui correspond à une indisponibilité d'environ 45 minutes par mois soit 9 heures par an.

- Le niveau de disponibilité des données stockées : celui-ci varie en fonction des services et des options retenues par le client.

Haute Disponibilité de l'information

Le système d'archivage électronique doit fonctionner durant les plages d'utilisation prévues par le contrat établi entre le client et le prestataire, et doit garantir l'accès aux services et aux archives avec le temps de réponse attendu.

Pour faire face à cet enjeu, le prestataire propose un plan de sécurisation à deux niveaux :

- Le Plan de Reprise d'Activité (PRA) qui permet un redémarrage à froid de l'activité après un sinistre, avec restauration du système d'archivage.
- Le Plan de Continuité d'Activité (PCA) qui permet une reprise à chaud par une redondance de l'infrastructure sur 1 ou 2 sites distants avec une réplication en temps réel des données (haute disponibilité sur 1 ou 2 sites).

Le PRA et le PCA ont pour objectif de minimiser les pertes de données et d'accroitre la réactivité en cas de sinistre majeur. Le PCA doit quasiment être transparent pour les utilisateurs, et doit garantir l'intégrité des données sans perte d'information.

Perte de données et/ou fuite de données

Pour contrecarrer les risques de perte de données et/ou de fuites de données, un ensemble de techniques de protection contre la fuite d'informations ont été développées.

Des techniques DLP (Data Loss Prevention) ou/et IRM (Information Right Management) peuvent être mises en œuvre à plusieurs niveaux :

- **Au niveau des réseaux** : avec des passerelles d'analyse des échanges de données (transfert de fichiers ftp et ftps, requêtes d'archivage via les protocoles http et https).
- **Au niveau des serveurs** : avec la surveillance des fichiers et des dossiers exposés, en signalant aux équipes de sécurité toute activité anormale ou tout utilisateur inhabituel.
- **Au niveau des données** : avec des algorithmes d'identification des données (mots clés, expressions régulières) pour identifier les données sensibles.

Ces techniques DLP ou/et IRM peuvent aider à assurer la conformité du service d'archivage sur le Cloud avec le cadre réglementaire et la directive de protection des données de l'Union Européenne.

Dépendance technologique vis-à-vis du fournisseur

Un des risques identifiés de l'archivage sur le Cloud est la dépendance technologique vis-à-vis du prestataire, c'est-à-dire l'impossibilité de changer pour un autre fournisseur ou pour revenir à une solution internalisée sans perte de données.

Ce risque peut être maitrisé par l'exigence contractuelle d'une clause de réversibilité et/ou d'interopérabilité La clause de réversibilité devra être accompagnée d'un plan de réversibilité détaillé.

Faillite, rachat du prestataire

En cas de faillite du prestataire d'archivage sur le Cloud, le client propriétaire des données archivées peut récupérer ses données à condition que celles-ci soient séparables de toutes autres données au moment de l'ouverture de la procédure de faillite du prestataire.

La question de l'accès à ces données archivées devra être précisée dans le contrat conclu entre le prestataire cloud et son client. (Voir également clause de réversibilité)

Pour faire face au risque de faillite d'un prestataire d'archivage en mode SaaS développant lui-même la solution logicielle, le client pourra exiger le dépôt des codes sources de l'application d'archivage électronique auprès de l'Agence de Protection des Programmes (APP).

Protection des données

1. Sécurité incombant au prestataire (politique de sécurité)

La politique de sécurité du prestataire doit reprendre la quasi-totalité des charges qui incombent au client dans ce périmètre :

- Accès au site,
- Accès aux serveurs,
- Accès aux applications.

En détail, ces aspects sont couverts comme suit.

La contrainte **d'accès aux sites** est double : préserver l'accès aux datacenters, où sont les serveurs, et aux bureaux du prestataire, où l'exploitation des serveurs est faite. Dans les deux contextes un **accès par badge personnel est nécessaire**. La surveillance des datacenters pour éviter le vol de matériel est très sévère : toute action de maintenance doit être planifiée à l'avance, des systèmes d'authentification biométrique ou autres technologies du même type sont souvent utilisés.

L'**accès au serveur** exige bien évidement une **authentification de chaque administrateur**, qui aura un **périmètre d'action limité**. Une fois vérifiée l'habilitation de l'administrateur, une application de monitoring peut enregistrer ses actions, afin de dissuader de toute action malveillante. Bien que cela ne soit pas une obligation, dans un contexte d'externalisation, s'assurer que ce type de moyen soit mis en œuvre est important.

Enfin, la gestion des **accès aux applications** se limite normalement la définition d'un administrateur applicatif chez le client. Ce dernier dispose d'un portail d'administration qui lui permettra de définir les habilitations et les droits d'accès de chaque utilisateur. Leurs actions sont donc souvent sous la responsabilité directe du client.

2. Protection des réseaux - Chiffrement des liaisons (protéger les transferts)

Dans la quasi-totalité des cas, le fournisseur d'un service Cloud assure une communication sécurisée vers les datacenters.

Comme déjà anticipé, quand le client exploite directement le serveur à distance (offre IaaS ou PaaS), une connexion VPN est mise en place pour protéger l'accès direct au réseau du serveur. Pour accéder à un service d'archivage (offre SaaS) le chiffrement de la communication (avec SSL) a force de règle de l'art et assure un accès aisé à l'utilisateur final (le navigateur rend transparent toute étape du protocole de sécurisation).

Afin d'assurer une facilité d'accès aux utilisateurs, le VPN peut aussi être employé, mais son utilisation reste réservée au versement ou transfert par lot des archives.

3. Chiffrement des archives (protéger les données).

Le chiffrement des données archivées peut, à première vue, paraitre la solution la plus sûre pour protéger des données. Cela est peut-être vrai dans le court terme, mais se révèle une contrainte très forte dans le domaine de l'archivage. En fait, la gestion des clefs et la durée de vie des algorithmes utilisés pour le chiffrement constituent des freins majeurs quand la donnée a vocation à être préservée à l'identique dans le long terme.

Il existe bien des domaines où le chiffrement des contenus est obligatoire (voir les données de santé). Dans ces cas de figure, le fournisseur propose des prestations complémentaires pour la gestion des clefs (coffre-fort numérique, utilisation de dispositifs de sécurité comme un HSM…), mais il existera toujours une « clef maitre » dont la pérennité et la sécurisation sera à la charge exclusive du client.

Les contraintes énoncées ci-dessus, complétées par des délais supplémentaires générés par le traitement des données, induisent une approche qui privilégie la protection de la 'donnée-trésor', plutôt que la dissimulation de cette dernière.

Les indispensables

1. Contrats. Clauses indispensables et minimales

L'archivage de contenus dans le cloud nécessite d'être attentif sur certaines clauses contractuelles. Pour en faciliter la compréhension juridique, il est conseillé d'utiliser des contrats rédigés en langue française.

Clause de localisation géographique des contenus.

Le prestataire du service Cloud doit préciser dans son contrat la localisation géographique des serveurs et des contenus archivés. L'utilisateur du service doit vérifier que contractuellement il a l'assurance que ses contenus archivés et externalisés seront situés, durant tout leur cycle de vie, sur le territoire de l'Union Européenne ou sur le territoire souverain.

La plus grande préoccupation par rapport à la localisation des données est dans l'application des règles de protection des données personnelles, et dans leur « export ». Le règlement européen qui pourrait remplacer dans quelque temps la directive actuelle de 1995 aura force de loi immédiate, c'est à dire sans besoin de transposition dans la loi de chaque pays de l'Union Européenne. Il serait souhaitable de disposer d'un dispositif attachant à un serveur ou à un « conteneur » une localisation géographique, un peu comme le ferait un système GPS, et de pouvoir lier ce dispositif aux logiciels d'archivage et de gouvernance.

Clause de traçabilité

Dans le cadre de la mise en œuvre de la norme NF Z42-013 et/ou d'une éventuelle certification liée à la marque NF 461, il est indispensable de prévoir une clause de traçabilité. Cette dernière doit être en mesure de certifier la mise en œuvre des journaux du cycle de vie des archives ainsi que des journaux des évènements du SAE. Ces journaux doivent comporter les informations obligatoires précisés dans le référentiel de certification de la marque NF 461 et/ou dans la norme NF Z42-013.

Clause de réversibilité et plan de réversibilité.

Il est important dès le début du contrat, de prévoir sa fin et tout particulièrement d'avoir la certitude qu'il sera possible de récupérer les contenus externalisés en fin de contrat ou dans le cas de la rupture du contrat. Il arrive parfois que les phases de rupture de contrat soient délicates. Pour éviter toute difficulté, il est possible de prévoir contractuellement **un plan de réversibilité** dès la mise en place du contrat.
Dans le cadre de la mise en œuvre de la norme NF Z42-013 et d'une éventuelle certification Marque NF 461, cette clause doit permettre de prévoir la capacité du prestataire à restituer les contenus, mais également les éléments de traçabilité associés aux contenus (journaux du cycle de vie des archives). Les journaux générés par le prestataire ne doivent comporter que des informations liées aux contenus archivés pour son client.

Clause liée au transfert des archives.

Pour préserver la confidentialité des contenus, il est important de vérifier que le contrat n'autorise le transfert des contenus archivés d'une zone géographique vers une autre que si elle est spécifiée contractuellement.

Bien entendu, il est également important de vérifier que tout transfert de contenu d'une zone de stockage à une autre est réalisé en garantissant la protection des contenus lors du transit.

Clause d'auditabilité.

Le contrat d'archivage sur le Cloud doit intégrer une clause organisant un audit par une société indépendante ou autorisant le client à organiser lui-même cet audit.

Dans ce cas, le prestataire serait tenu de corriger les écarts observés par rapport aux engagements contractuels et règlementaires. La périodicité de l'audit devrait être a minima annuelle.

Les audits permettront de vérifier notamment les points suivants :

- Les mesures de sécurité mises en œuvre par le prestataire d'archivage électronique,
- Les journaux relatifs à la gestion du cycle de vie des archives,
- Les mesures mises en place pour sauvegarder ou supprimer les archives, pour prévenir toutes transmissions illégales, pour empêcher le transfert vers un pays non autorisé.

L'audit doit permettre de s'assurer que les mesures de sécurité et de confidentialité mises en place ne peuvent être contournées.

Depuis le 17 décembre 2012, l'audit des Systèmes d'Archivage Electronique peut faire l'objet d'une certification NF 461 délivrée par Afnor Certification.

Dans certains domaines professionnels, des contraintes règlementaires viennent s'ajouter, comme par exemple :

- Les normes du Comité français d'organisation et de normalisation bancaires du **CFONB**, qui a pour mission de normaliser les échanges et l'archivage sécurisé des systèmes de paiement.
- Les flux d'encaissement avec l'application au 1er janvier 2014 du **SEPA** et l'obligation de gérer et conserver les mandats.
- **Bâle II et Bâle III** ont pour objectif de renforcer la sécurité du système financier par une meilleure gestion des risques, notamment ceux qui concernent les sites d'hébergement des données.
- **Solvabilité II** (Solvency II) est une réforme réglementaire européenne du monde de l'assurance. Pour répondre aux objectifs de Solvabilité II, les compagnies d'assurance et de réassurance doivent :
  - Définir une politique de gouvernance de l'information dans laquelle doit être prise en compte l'archivage,
  - Disposer de pistes d'audit exhaustives, intègres et lisibles,
  - Mettre en œuvre un archivage sécurisé des flux de données et des documents.
- **21 CFR Partie 11** est une réglementation émise par la FDA (Food and Drug Administration) américaine. Cette norme consiste à s'assurer que les enregistrements et les signatures électroniques sont équivalents à des enregistrements sur papier et à des signatures manuscrites.
- **L'hébergement de données de santé à caractère personnel** est encadré en France depuis la loi N°2002-303 du 4 mars 2002 dans le but de garantir la confidentialité, l'intégrité et la disponibilité des données des patients. Ce texte soumet cette activité d'hébergement à un agrément préalable du Ministre de la Santé.

Clause liée à une requête des autorités administrative et judiciaire

Si une requête provenant d'une autorité administrative ou judiciaire est reçue par le prestataire de service cloud, ce dernier s'engage à en informer systématiquement et immédiatement son client.

Clause liée à la compétence juridique du contrat.

Le contrat doit préciser la loi qui s'applique ainsi que les tribunaux compétents en cas de litige.

Clauses abusives à éviter

- Révision de contrat unilatéralement

  Dans certain cas, certains articles sont ajoutés dans les contrats pour permettre une modification contractuelle « unilatérale ». Il arrive d'avoir des clauses qui précise que le prestataire pourra à tout moment modifier certaines dispositions contractuelles prenant effet dès lors qu'elles sont publiées sur le site du prestataire. D'après une tribune publiée par Maître Olivier ITEANU le 11 octobre 2013 sur le site Eurocloud, ce type de clause est souvent positionné en fin de contrat.

2. Elimination et restitution (élément de preuve, certificat)

L'archivage doit être mené dans le respect des obligations légales et réglementaires. En particulier les données et documents doivent avoir été conservés pendant le temps requis de conservation et seulement pendant ce temps.

Dans des positions de "défense", comme des requêtes des autorités de tutelle, des requêtes judiciaires voire des contentieux, l'entreprise peut être amenée à démontrer que :

- les données devant être détruites l'ont bien été (exemple des données à caractère personnel dans le cadre du droit à l'oubli),
- les données ayant été détruites pouvaient effectivement l'être et qu'il est légal de ne pas les fournir (sincérité et non dissimulation).

A cet égard, la preuve des éliminations doit être tracée dans les journaux et les certificats d'élimination eux-mêmes archivés.

Ces dispositions restent bien évident applicables pour un système d'archivage partiellement ou totalement dans le cloud et doivent figurer dans le SLA.

De même, en cas de restitution des données, qu'il s'agisse d'une restitution des données lors d'un changement du prestataire de stockage ou d'une restitution des données lors d'une cession d'activités, il importe d'avoir la garantie que les données restituées sont bien éliminées et ne peuvent plus être accessibles d'aucune manière.

Dans le cas contraire, les risques peuvent être de nature variable. La fuite de données confidentielles, concurrentielles est l'un des risques évident auquel on pense en premier lieu mais ce n'est pas le seul.

Dès lors qu'elles existent toujours, des données peuvent être utilisées dans des procédures judiciaires même si leur durée de conservation était écoulée. La responsabilité de l'entreprise peut de ce fait être engagée.

3. La réversibilité sur le Cloud

On désigne par « réversibilité » la capacité qu'a un opérateur (tiers-archiveur par exemple) de restituer à leurs propriétaires les archives numériques qui lui ont été confiées en en garantissant la valeur et l'intégrité. Par archives numériques on entend ici toutes les pièces numériques constituant le « paquet » d'archives et dont on a défini au préalable le contenu entre les contractants.

Les cas de récupération des contenus peuvent être multiples : changement de prestataire, cession d'une activité, recours momentané à un tiers en attendant de se doter de son propre système d'archivage, etc.

Quelles sont les obligations auxquelles devraient souscrire un fournisseur d'espace dans le cloud pour garantir cette réversibilité ?

En tout état de cause, il s'agit de respecter une correspondance entre ce qui a été versé et ce qui doit être restitué, nonobstant les événements qui auraient pu avoir lieu dans l'intervalle de temps entre le versement et la restitution (ces événements peuvent être divers ; il peut y avoir eu par exemple destruction, auquel cas il faut pouvoir expliquer pourquoi le volume restitué n'est pas identique au versement initial). Dans tous les cas, ces événements doivent être tracés, et le prestataire doit pouvoir fournir des journaux de traçabilité.

Le fournisseur doit donc offrir contractuellement un certain nombre de prestations techniques et fonctionnelles qu'il s'engage à garantir pendant toute la durée de la prestation.

On distinguera le fait que, en mode IaaS, le prestataire doive garantir une disponibilité d'accès technique pour que le client puisse lui-même récupérer ses contenus en vidant les espaces de stockage qui lui avaient été alloués (il ne s'agit pas alors de réversion incombant au prestataire, au sens strict), et le mode SaaS, dans lequel le prestataire doit être capable de mener des opérations de réversion complètes et sécurisées.

- **Questions à se poser en termes de réversibilité, dans le choix d'un fournisseur.**
  - Quels sont les délais de restitution ?
  - L'engagement du prestataire à respecter sa politique d'archivage.
  - Quels sont les coûts associés à la prestation ?

4. La traçabilité - audit et certification du prestataire

D'une manière générale, la traçabilité est devenue un enjeu industriel et commercial important quelle que soit l'activité. Elle répond à des exigences de réglementation et permet de suivre l'activité d'une entreprise à travers le suivi de ses approvisionnements, de ses processus, de ses produits, de leur stockage, de leur acheminent. Naturellement ce suivi s'effectue via des applications, des ensembles de données, des documents, ce qui adresse une première acception de la traçabilité liée au document.

Mais, plus particulièrement en ce qui concerne l'archivage du document numérique ou de la donnée, on, vise, grâce à la traçabilité, à assurer le suivi de toutes les opérations effectuées, en accompagnant le déroulement du cycle de vie de l'archive : sa prise de valeur (signature, horodatage), son versement, les opérations de conversion de formats, de migrations de supports qu'il peut subir, les opérations de communication, d'élimination/destruction, etc.

On peut même dire que la traçabilité est une caractéristique[5] de l'archive, puisque c'est un des éléments qui vont permettre de garantir le caractère engageant des documents, contrairement à ce qui se passe dans une Ged par exemple. Garantir la trace d'une date d'entrée dans un système, d'une opération de migration, d'une opération de destruction c'est assurer la qualité sur les autres critères qui définissent l'archivage : pérennité, intégrité, sécurité, imputabilité (attribution à un auteur). La traçabilité fait ainsi partie des six conditions qui doivent être assurées par une activité d'archivage numérique[6].

La traçabilité doit avoir un caractère systématique et contribuer à enregistrer tous les événements qui ont pu affecter le fonctionnement du système ou les documents. Cette traçabilité s'exprime elle-même par la journalisation et donc produit le journal des événements, qui est lui-même un document à vocation probatoire.

Par rapport à un archivage dans le Cloud, il conviendra de prendre en compte contractuellement les éléments suivants :

- Ce qui témoigne du versement du document (date, heure, qui le fait),
- Trace d'une activité de conversion : à partir de quel format, vers quel format, quantité de données ou de documents impactés, durée de l'opération, relevé des incidents éventuels au cours de la conversion…

---

5 CHABIN Marie-Anne, Nouveau glossaire de l'archivage, février 2010 http://extranet.ucanss.fr/contenu/public/EspaceDeveloppementDurable/pdf/Nouveau_glossaire_de_l_archivage.pdf

6 Cf. Aproged, Guide archivez numériquement vos documents, Paris

- Trace d'une activité de changement de support : quelle décision, de quel support à quel support, date et heure de l'opération, quantité de données ou de documents impactés, durée de l'opération, relevé des incidents éventuels au cours de la migration…
  Nota Bene – Ici on peut se demander de quelle traçabilité relève les changements que le fournisseur de service opère sur les documents et données dans le cadre de sa politique d'optimisation des serveurs.
- Traces des opérations de communication : qui, pour qui ? date et heure.
- Traces des opérations de destruction : qui, pour qui ? avec quelles méthodes, date et heure, relevés de destruction.
- Sous quelle forme le fournisseur de service assure-t-il la traçabilité ? où est l'outil de journalisation : IaaS, Saas ? Qu'est-ce qui est restitué ? Qu'est-ce qui est consultable, par qui, à quel moment ?
- Comment assurer l'historique de la traçabilité (l'archive de l'archive…) ?

III. Normes - certification - Perspectives pour la France

Norme NF Z42013 et ISO 14641-1

1. Du juridique au technique

D'un point de vue juridique un système d'archivage électronique doit, pour le moins, garantir aux documents conservés fidélité, intégrité, pérennité et sécurité pour que ceux-ci puissent disposer d'une valeur probatoire et être admissibles lors d'une procédure.

Garantie d'intégrité suppose que le document ne pourra subir aucune modification volontaire ou malveillante durant sa période de conservation.

Un document est considéré comme fidèle au document d'origine s'il permet de reconstituer toute l'information nécessaire aux usages auxquels le document d'origine était destiné. Ce concept est utilisé en cas de rupture incluant notamment une numérisation ou une conversion de format.

La pérennité réside dans la garantie du système à restituer de façon intelligible un document électronique tout au long de sa période de conservation.

La conformité d'une solution d'archivage électronique à cette norme permet de garantir que celle-ci est conçue et utilisée suivant les règles de l'art. Cette particularité peut être interprétée comme la conséquence d'une jurisprudence de 1976.

Pour atteindre ces objectifs lors de la mise en place d'un système d'archivage électronique, il convient d'utiliser un éventail de dispositifs techniques dont les caractéristiques et l'organisation sont spécifiées par la norme AFNOR homologuée NFZ42-013 ou sa version ISO 14641-1.

2. La norme NFZ42-013 – Aspects essentiels

La version actuelle date de mars 2009[7] après une première version publiée en juillet 1999 et une révision publiée en Décembre 2001. Dans la version 2009, la norme apporte des réponses claires concernant l'élargissement du périmètre des objets numériques susceptibles d'être pris considération et sur la nature des supports mis en œuvre par les systèmes d'archivage électronique.

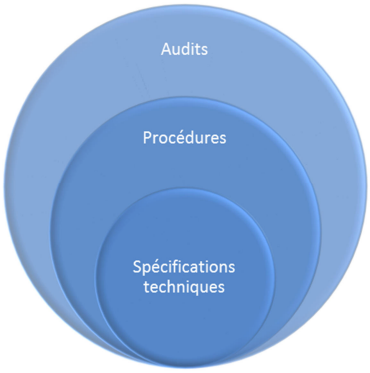
C'est ainsi que désormais, outre les écrits (au sens de la loi du 13 Mars 2000), les objets sonores, les séquences vidéo, les dessins ou les plans 2D ou 3D ainsi que les images médicales entrent dans le champ d'application de la norme révisée. Ces objets pouvant être créés directement sous forme numérique ou provenir de processus de conversion à partir de supports analogiques (papier, microfilm, bandes, etc..).

[7] La version ISO 14641-1 a été publiée en Janvier 2012 – Il s'agit d'une traduction en anglais de la norme NFZ42-013 où ne figurent que quelques adaptations sémantiques afin de prendre en compte les pratiques anglo-saxonnes.

L'autre apport décisif corrige l'aspect restrictif de la version précédente en prenant en compte toutes les natures de supports informatiques susceptibles d'être utilisés pour archiver les documents : supports fixes ou amovibles, de type WORM physique ou logique, ou simplement réinscriptibles.

Trois niveaux de spécifications

Les spécifications décrites dans la norme concernent exclusivement les systèmes informatiques destinés à conserver des documents électroniques dont l'archivage électronique fait partie. Elles sont organisées en trois couches concentriques :



- Les spécifications du système,
- Les procédures,
- Les audits.

De façon plus détaillée cette organisation conduit à la structure suivante du document normatif :

Le cadre global et les généralités concernant notamment :

- Le domaine d'application,
- Les références normatives connexes applicables,
- Les définitions des termes employés,
- Les principes de base et les options.

Les spécifications proprement dites concernant :

- Le système informatique,
- Les sécurités,
- Les procédures d'exploitation,
- Le suivi des procédures.

Les conditions de mise en œuvre comprenant :

- Les audits réguliers,
- L'utilisation éventuelle de tiers archiveur,
- Le recours à des prestataires de services,
- Les options destinées à renforcer la sécurité du système.

3. Révision éventuelle de la NFZ42-013

La règle et la pratique de l'AFNOR veulent que les normes soient proposées à la révision tous les cinq ans. . La publication actuelle de la norme datant de Février 2009, sa révision sera à l'ordre du jour du comité technique de la CN 171 en 2014.

Le comité technique peut ainsi décider s'il y a lieu de revoir tout ou partie des spécifications si les pratiques du marché ou les évolutions techniques rendent difficiles ou impossibles l'application d'une norme.

Cette réflexion a débuté notamment dans le cadre de la création d'une famille de normes concernant le domaine de l'archivage électronique dont la NFZ42-013 serait « l'enveloppe ». Dans cette famille serait alors incluses toutes les normes existantes ou à venir ayant un rapport avec le domaine.

Au stade actuel des travaux préliminaires, le comité technique n'a pas estimé que les conditions étaient réunies pour lancer concrètement le processus de révision.


Le Cloud comme nouveau moyen d'archiver pourrait être un des sujets pouvant motiver le comité à réflechir à une révision de la norme.

Marque NF 461

La certification NFZ42-013 des Systèmes d'Archivage Electronique (SAE)

Compte tenu de l'importance qu'a prise au fil du temps la normalisation NFZ42-013 des systèmes d'archivage électronique, la reconnaissance de leur conformité devenait une demande récurrente de la plupart des organisations ayant entrepris cette démarche.

A l'initiative de différentes associations parmi lesquelles l'APROGED qui a eu une position de leader, un groupe de travail a été mis en place par AFNOR Certification auquel s'était joint le SIAF (Service Interministériel des Archives de France) afin de définir les régles et le référentiel d'audit des SAE afin d'en déterminer le niveau de conformité au regard de la norme NFZ42-013.

Les productions de ce groupe de travail ont été suivies et contrôlées par la commission AFNOR CN171 responsable des travaux sur la norme NFZ42-013.

A l'issue de ce processus de certification et dans la mesure où le résultat de l'audit est satisfaisant, les SAE peuvent se voir attribuer une marque de qualité. Il s'agit en l'occurrence de la marque NF461.

Par ailleurs, le ministère de la Culture a mis en place un dispositif d'agrément pour les prestataires d'archivage papier et numérique pour la conservation des archives publiques courantes et intermédiaires (décret n°79-1037 du 3 décembre 1979 modifié relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques et loi n° 2008-696 du 15 juillet 2008 sur les archives), pour lequel il est demandé aux prestataires d'être conformes à des normes dont la norme Z 42-013 dans sa version de mars 2009 pour les archives numériques.

Dans ce contexte, la démarche de mise en conformité à la norme NFZ42-013 des SAE et des prestataires d'archivage devenait incontournable en s'appuyant notamment sur l'intervention d'organismes, agréés par le Cofrac (Comité Français d'Accréditation), désigné comme unique instance nationale d'accréditation par le décret du 19 décembre 2008.

Les enjeux et la démarche

La démarche de certification permet d'une part de certifier des systèmes d'archivage électronique et, d'autre part, des prestataires qui peuvent se voir attribuer la marque NF342 (Prestations d'archivage et de gestion externalisée de documents) sur la gamme « Support papier » s'ils sont certifiés sur la base de la norme NFZ40-350 ou la marque NF461 sur la gamme « Documents électroniques » sur la base de la norme NFZ42-013, version 2009.

La certification des SAE sur la base de la norme NFZ42-013 est dorénavant prononcée soit dans le cadre de systèmes opérés par des prestataires qui sont alors éligibles à la marque NF Services, soit dans le cadre de systèmes internes opérés par des entreprises ou des organismes.

De par son ciblage métier et une approche dépassant les seuls aspects sécuritaires, la démarche de certification NFZ42-013 des SAE doit apporter une meilleure lisibilité des utilisateurs quant à la fiabilité de l'archivage électronique auquel ils ont recours notamment dans sa dimension probatoire.

Evolution du cadre juridique et réglementaire

Le cadre juridique et réglementaire français est actuellement le frein majeur à l'évolution des pratiques et des usages des entreprises liées à l'archivage des documents numériques dans le Cloud.

Même si de nombreux documents anciennement produits sous forme papier sont de plus en plus numériques nativement, la masse de documents papiers échangée dans des cadres réglementaires reste importante. Dans certains domaines, la France a été capable de faire évoluer ces dix dernières années sa réglementation pour favoriser les échanges de documents numériques. Des pays européens voisins enrichissent actuellement leur arsenal règlementaire et légal pour permettre de mieux encadrer l'usage du cloud et la maitrise des risques. La France est également en marche mais le chemin à parcourir pour permettre l'archivage « *légal* » sur le cloud reste encore long et incertain.

1. Le Luxembourg encadre la faillite des acteurs du Cloud

D'autres pays européen plus petits que la France tel que le Luxembourg, sont bien plus actifs et dynamiques en matière de réforme liée à l'économie numérique. Plusieurs initiatives ont été mises en œuvre ces cinq dernières années pour définir un cadre juridique et règlementaire étendu afin de développer la pratique de l'archivage des documents dans le Cloud.

Récemment (11 juin 2013), le Luxembourg a voté une loi instaurant le **droit de revendication** en faveur de la personne qui a confié ses données auprès d'un **fournisseur de solutions "cloud" qui est tombé en faillite**. C'est par un amendement à l'article 567 du Code du Commerce que le Luxembourg montre l'exemple à l'Europe.

2. Nouvelle équation au Luxembourg : Document numérisé ←→papier

Comme pour la France avec l'arrivée de la marque NF 461 sur les systèmes d'archivage électronique, un groupe de travail Luxembourgeois a œuvré à la définition d'un référentiel de certification d'un Système d'Archivage Electronique afin de permettre la certification d'acteurs de la dématérialisation et/ou de l'archivage.

Ces travaux ont donné lieu à un nouveau statut de « **PSDC** », sociétés Luxembourgeoises certifiées sur un référentiel ILNAS (Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services).

Il s'agit d'un « Statut attribué par l'ILNAS à une personne morale exerçant à titre principal ou secondaire, pour ses propres besoins ou dans le cadre de services proposés à ses clients, des processus de dématérialisation ou de conservation formellement reconnus par l'ILNAS comme conformes aux exigences et aux mesures définies dans la règle technique d'exigences et de mesures pour la certification des Prestataires de Services de Dématérialisation ou de Conservation (PSDC)[8]. »

Pour appuyer cette certification, le Luxembourg a souhaité également proposer une modification du cadre réglementaire liés aux documents financiers en proposant **un projet de loi relatif à l'archivage électronique** et modifiant la loi modifiée du 5 avril 1993 relative au secteur financier. Ce projet de loi a été analysé par le Conseil d'Etat donnant lieu le 8 octobre 2013 à un rapport d'examen des articles du projet.

En résumé, le Conseil d'Etat a formulé un avis dont voici les principales remarques :

- **Cadre légal** : Pourquoi traiter de la question de la valeur probante des documents conservés sous forme numérique dans un régime légal à part (financier) plutôt que dans le Code civil et dans le code du commerce?
- **Périmètre documentaire** : Pourquoi exclure du périmètre les documents administratifs ?
- **Périmètre temporel** : Comment gérer légalement la différence entre un document dématérialisé avant la modification de la loi (donc sous le régime du règlement grand-ducal du 22 décembre 1986) et un document dématérialisé par application de la nouvelle loi ?
- **Périmètre du PSDC** : Ne faut-il pas distinguer les PSDC qui œuvrent pour leur propre compte (archivage internalisé) de ceux qui œuvrent pour le compte d'autrui ?
- **Cadre national et européen** : Ne faut-il pas se poser la question de la légalité des documents dématérialisés au-delà du contexte national en positionnant la problématique au moins au niveau européen ? En effet, que vaudrait un document dématérialisé produit par le Luxembourg dans un pays ayant une loi différente et ne reconnaissant pas le document dématérialisé.

[8] Définition de PSDC (**Prestataire de Services de Dématérialisation ou de Conservation**) par l'ILNAS (L'**I**nstitut **L**uxembourgeois de la **N**ormalisation, de l'**A**ccréditation, de la **S**écurité)

Bien que le projet de loi du Luxembourg ne soit pas abandonné, les avis rendus par le Conseil d'Etat soulèvent bien la difficulté de légiférer sur le sujet lié à la vocation probatoire des documents papiers dématérialisés et à leur archivage indépendamment de la problématique Cloud.

3. Que fait la France

Fort de ce constat et de ces expériences du Luxembourg, l'APROGED a mis en place depuis plusieurs mois un groupe de travail intitulé « ELIMDOC » afin de réfléchir aux règles légales que la France pourrait adopter pour permettre la mise en œuvre d'une économie de confiance autour du document dématérialisé pour passer de **l'archivage à vocation probatoire** à **l'archivage légal et pourquoi pas, sur le Cloud**.

Un premier constat est déjà mis en évidence. La France ne pourra pas légiférer sur le sujet sans **s'inscrire dans un périmètre européen**. Les efforts du Luxembourg et l'avis du Conseil d'Etat montrent bien que les actions nationales ne pourront avoir un véritable effet que dans un cadre harmonisé au moins à l'échelle de l'Europe.

La CNIL a également œuvré autour du Cloud et a publié des **recommandations** pour les entreprises et les particuliers qui envisagent de souscrire à des services sur le Cloud. Même si ces avis ne sont pas exclusivement orientés vers l'archivage des documents sur le Cloud, la prise en compte de ces recommandations rappelées en partie dans ce livre blanc sont incontournables.

4. La facture électronique en France

Pour certains types de document, la France a été active afin de permettre la mise en place d'une économie dématérialisée des documents et améliorer ainsi la compétitivité des entreprises. C'est le cas par exemple de la **facture électronique** qui est encadrée par une législation fiscale (articles 289 bis et 289 V du code général des impôts). Cette évolution s'est inscrite sur la base d'une transposition nationale d'une directive européenne. Elle permet aux entreprises de dématérialiser les factures dès lors que les garanties d'authenticité, de non répudiation, et d'intégrité sont respectées.

Les **factures électroniques sont des documents qu'il est possible d'archiver sur le cloud** dès lors que les différents points soulevés dans ce livre-blanc et dans le code général des impôts sont pris en compte et respectés.

5. Les archives publiques

Dans le **secteur public**, le décret N° 2009-1124 du 17 septembre 2009 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques a explicitement souhaité définir un cadre réglementaire reposant sur un **agrément** et respectant les **règles de l'art normatives**. Cette évolution par rapport au décret N° 79-1037 de 1979 est un signe fort de l'administration mais se limite au périmètre de la sphère publique.

L'article 20.5 précise : « Toute personne physique ou morale souhaitant assurer la conservation d'archives publiques et bénéficier de l'agrément prévu au II de l'article L. 212-4 du code du patrimoine doit remplir les conditions suivante :

1° Exercer son activité en **conformité avec les normes** relatives aux prestations en archivage et gestion externalisée de documents sur support papier ainsi que celles relatives à l'archivage électronique, déterminées par arrêté du ministre chargé de la culture ;

2° **Conserver sur le territoire national les archives qui lui sont confiées**, dans des locaux conformes aux prescriptions de la direction des Archives de France ;

3° Recourir à des **professionnels qualifiés** en matière de **sécurité** et de **conservation matérielle** des archives ;

4° Assurer une **conservation sécurisée**, incluant une **politique de confidentialité**, destinée notamment à assurer la protection contre les accès non autorisés ainsi que **l'intégrité** et la **pérennité** des archives ;

L'article 20-11 précise que l'agrément est accordé pour une durée de cinq ans ; ce délai est ramené à **trois ans** lorsqu'il est accordé, même pour partie, pour conserver des archives sur support numérique.

 Les **archives publiques semblent donc être des documents qu'il est possible d'archiver sur le cloud** dès lors que les différents points soulevés dans ce paragrpahe et dans ce livre blanc sont respectés.

CONCLUSION

Les motivations des entreprises pour «aller dans le Cloud » peuvent être variées. Elles peuvent être **d'ordre financier** ; **technique** (externaliser son système informatique pour éviter les coûts de maintenance, éviter également la gestion et la mise à jour d'un parc d'applications logicielles) ; **organisationnel** (permettre à des entreprises étendues ou à des groupes de partager virtuellement plates-formes et applications…) ; **lié à la volumétrie** des applications et des contenus.

L'approche du Cloud peut être **globale** (externaliser un maximum d'activités) ou **partielle** (se concentrer sur un aspect de la chaîne du traitement de l'information).
Dans tous les cas, il importe de bien mesurer les avantages et les inconvénients de ces choix.

Dans ce livre blanc, nous nous sommes concentrés sur un des aspects de la chaîne du cycle de vie du document : **l'archivage**. A priori, on pourrait penser que cette étape rentre dans le cadre d'une externalisation seulement partielle des activités (par exemple pour des raisons de volume et de coûts de stockage, on ne choisit d'aller dans le cloud QUE sur la partie archivage de la chaîne de valeur) ; mais il y a malgré tout un degré de complexité complémentaire car l'archivage est une activité dont les modalités et le caractère contraignant sont très particulières. Elle implique notamment de déléguer à des tiers des responsabilités, que l'on maîtrise bien dans le domaine du service traditionnel, mais qui ne sont pas encore toutes pensées ou assumées par tous les acteurs du « cloud ».

C'est pourquoi nous avons voulu, dans le cadre de cette première réflexion, recenser l'essentiel des points critiques à aborder et à maîtriser avant de se lancer dans le choix d'un opérateur du cloud à qui l'on souhaiterait confier des tâches d'archivage et ses archives mêmes.

Dans un domaine encore fort mouvant, il conviendra d'être à l'écoute des retours d'expérience et d'améliorer et de compléter ces premières réflexions.

L'Aproged, en tant qu'association professionnelle, s'y emploiera.

ANNEXES

Annexe 1 : Terminologie - définition

- **AV -** Analyse de la valeur

  L'**analyse de la valeur** (**AV**) est une méthode rationnelle d'optimisation d'un « produit » (ou d'un procédé, un processus, un service). Le but de cette méthode est de concevoir un « produit » parfaitement adapté aux besoins de son utilisateur et ce, au coût le plus faible.

  Elle améliore donc la qualité d'un « produit » sans en augmenter le coût ou diminue le coût du produit sans réduire le niveau des services attendus.

  Le « produit » peut-être un produit existant ou nouveau, simple ou complexe, répétitif ou unique, mais peut être aussi un processus administratif ou industriel, un service interne à une entreprise ou vendu par cette entreprise. La méthode peut donc s'appliquer dans toutes les entreprises, l'ensemble des services et tous les secteurs économiques. Lorsqu'il s'agit d'analyse de la valeur de produit, on parle de *« value analysis »* ; lorsque c'est de l'analyse de la valeur en conception, de *« value engineering »* et enfin, pour de l'analyse de la valeur en gestion, on parle de *« value management »*.

- **BCR -** Binding Corporate Rules

  Les Binding Corporate Rules (BCR) désignent un code de conduite interne qui définit la politique d'un groupe en matière de transferts de données personnelles hors de l'Union européenne.
  Les BCR doivent être contraignantes et respectées par toutes les entités du groupe, quel que soit leur pays d'implantation, ainsi que par tous leurs salariés.
  Les BCR constituent une alternative aux Clauses Contractuelles Types puisqu'elles permettent d'assurer un niveau de protection suffisant aux données transférées hors de l'Union européenne.

- **CNIL**

  Commission nationale de l'informatique et des libertés. Site internet : www.cnil.fr

- **CSB –** Cloud Service Brokers.

  Société proposant des services Cloud intégrés via l'agrégation, l'intégration et le paramétrage de services Cloud existants.

- **CST -** Contrôle scientifique et technique

  Contrôle scientifique et technique (CST) de l'État sur les archives publiques.

- **DUA -** Durée d'utilité administrative

  La durée d'utilité administrative (DUA) est la durée pendant laquelle les documents, données ou informations archivés doivent être conservés et gardés en état d'être consultés et utilisés, soit par ceux qui les ont produits, soit par des services d'archives.

- **ECM -** Entreprise content management ➔Gestion de contenu.

- **FISA -** Foreign Intelligence Surveillance Act

  Le Foreign Intelligence Surveillance Act (FISA) est une loi du Congrès des Etats-Unis d'Amérique de 1978 décrivant les procédures des surveillances physiques et électronique, ainsi que la collecte d'information sur des puissances étrangères soit directement, soit par l'échange d'informations avec d'autres puissances étrangères.

- **ILNAS**

  Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité

- **ITAR** - International Traffic in Arms Regulations

  La Réglementation américaine sur le trafic d'armes au niveau international (en anglais *International Traffic in Arms Regulations*, ITAR) désigne un ensemble de règlements du gouvernement fédéral américain servant à contrôler les importations et exportations des objets et services liés à la défense nationale, tels que recensés sur la Liste des matériels de guerre et assimilés américains. Ces règlements s'appliquent tant au niveau des matériels qu'aux documentations associées.

- **HADS -** Hébergeur Agréé de Données de Santé.

- **Indexation**

  Processus permettant de définir des mots pour retrouver des contenus basé sur ces mots.

- **Métadonnées**

  Données permettant de décrire et de qualifier d'autres données ou contenus.

- **Patriot Act**

  Le **USA PATRIOT Act** (acronyme traduisible en français par : « Loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme ») est une loi antiterroriste qui a été votée le 26 ocotbre 2001.

  Dans la pratique cette loi autorise les services de sécurité à accéder aux données informatiques détenues par les particuliers et les entreprises, sans autorisation préalable et sans en informer les utilisateurs.

- **Principe du Safe Harbor**

  Il s'agit d'un ensemble de principes de protection des données personnelles publié par le Département du Commerce américain, auquel des entreprises établies aux Etats-Unis adhèrent volontairement afin de pouvoir recevoir des données à caractère personnel en provenance de l'Union européenne.
  Ces principes, négociés entre les autorités américaines et la Commission européenne en 2001, sont essentiellement basés sur ceux de la Directive 95/46 du 24 octobre 1995 :
  - information des personnes,
  - possibilité accordée à la personne concernée de s'opposer à un transfert ou à une utilisation des données pour des finalités différentes,
  - consentement explicite pour les données sensibles,
  - droit d'accès et de rectification,
  - sécurité des données,

  Le Safe Harbor permet donc d'assurer un niveau de protection suffisant pour les transferts de données en provenance de l'Union européenne vers des entreprises établies aux Etats-Unis.

- **PSDC**

  Prestataire de Services de Dématérialisation ou de Conservation au Luxembourg

- **RGI**

  Le RGI est un cadre de recommandations référençant des normes et standards qui favorisent l'interopérabilité au sein des systèmes d'information de l'administration. Le RGI est défini dans l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administrative

- **SAE**

  Système d'Archivage Electronique

- **SEDA**

  Standard d'Échange de Données pour l'Archivage. Le SEDA est basé sur des schémas XML. Il est intégré dans le RGI, qui le recommande pour tout échange entre un service d'archive et ses partenaires.

- **SLA -** Service Level Agreement

  Le **service level agreement** (SLA) que l'on peut traduire par "contrat du niveau de service" est un document qui définit la qualité de service requise entre un prestataire et un client.

Annexe 2 : normes, référentiels, guides et sources

Cette annexe établit une liste des normes, de textes et de sources en relation avec les sujets traités. Du fait du grand nombre de travaux et de normes dans les domaines abordés, cette liste est restreinte et n'est pas exhaustive. Nous vous conseillons également les guides de bonnes pratiques qui reprennent par sujet les différents travaux spécifiques à chaque sujet.

1. Guides APROGED[9]

- **Document & Cloud computing** – Guide de bonnes pratiques à l'attention des organisations françaises ou européennes. Editeur APROGED, juin 2012.
- **Archivez numériquement vos documents –** Editeur APOGED en partenariat avec Alliance TICS et le MDEF.

2. Normes et référentiels AFNOR et ISO

- **NF Z42-013 2009** (publication AFNOR Certification) **:** Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes.
- **ISO 14641-1** (issue de la norme NF Z42-013) : décrit les mesures techniques et organisationnelles à mettre en œuvre pour l'enregistrement, le stockage et la restitution de documents électroniques, afin d'en assurer la conservation et l'intégrité.
- **Marque NF 461 :** Référentiel de certification des Systèmes d'Archivage Electronique basé sur la norme NF Z42-013 et ISO 14641-1.

3. Autre livre blanc sur la certification des SAE.

- **Marque NF 461** : « *Comment certifier votre système d'archivage électronique* ». Editeur EVER TEAM, septembre 2013.

[9] Toutes les publications sont disponibles sur le site de l'APROGED : http://www.aproged.org

4. Autres textes de référence et sources

- **AFDEL** – Livre blanc - Cloud Computing - Une feuille de route pour la France
- **CR2PA** - Livre blanc – Politique d'Archivage, guide méthodologique. Publié en 2011
- **CNIL**
  - Coffre-fort numérique ou électronique Données Délibération N° 2013-270 du 19 septembre 2013.
  - « Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing » : http://goo.gl/eH3aF3
- **IDC France** : communiqué de presse de mars 2013.
- **Luxembourg**
  - Révision article 567 du code du commerce : http://goo.gl/bFyaxO
  - Projet de loi relatif à l'archivage électronique et modifiant la loi modifiée du 5 avril 1993 relative au secteur financier. Avis du Conseil d'Etat : http://goo.gl/OaYme4
- **Banque de France** – Autorité de Contrôle Prudentiel - Les risques associés au Cloud Computing – 07/2013
- **Cedhys – Fedisa** – L'archivage électronique pour les laboratoires pharmaceutiques – 06/2010
- **Sources Sénat :**
  - http://www.senat.fr/colloques/colloque_cnil_senat/colloque_cnil_senat_mono.html
  - Rapport « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information »
  - http://www.senat.fr/rap/r08-441/r08-441_mono.html
  - http://www.senat.fr/rap/r08-441/r08-44128.html
- **Autres sources**
  - Wikipedia : Solvency, Bâle.
  - légifrance.gouv.fr,
  - cfonb.org,
  - Blog Ever Team http://blog.ever-team.com
  - Gartner - Cloud Services Brokerage (CSB) : http://www.gartner.com/it-glossary/cloud-services-brokerage-csb

ENTREPRISES CONTRIBUTRICES

L'APROGED souhaite remercier les entreprises qui ont contribué à la réalisation de ce document et tout particulièrement :

- Philippe CHANTIN, **OUROUK**
- François CHAZALON, **RSD**
- Dominique COTTE, **OUROUK**
- Eric DESCOURS, **TESSI**
- Christian DUBOURG, **EVER TEAM**
- Jean MOURAIN, **RSD**
- Gérard WEISZ, **SIRIUS SYSTEMS**
- Oscar WOLLMAN, **DOC@WORK**

Animateur du groupe de travail Aproged : Christian DUBOURG - Secrétaire APROGED

www.ever-team.com

www.docatwork.fr

www.rsd.com

www.ourouk.fr

www.sirius-system.com

www.tessi.fr

Mail : contact@aproged.org
Site web : www.aproged.org

www.aproged.org

Une publication APROGED – Janvier 2014

Création : APROGED – Suzanne NUNES

Conseil en management de l'information

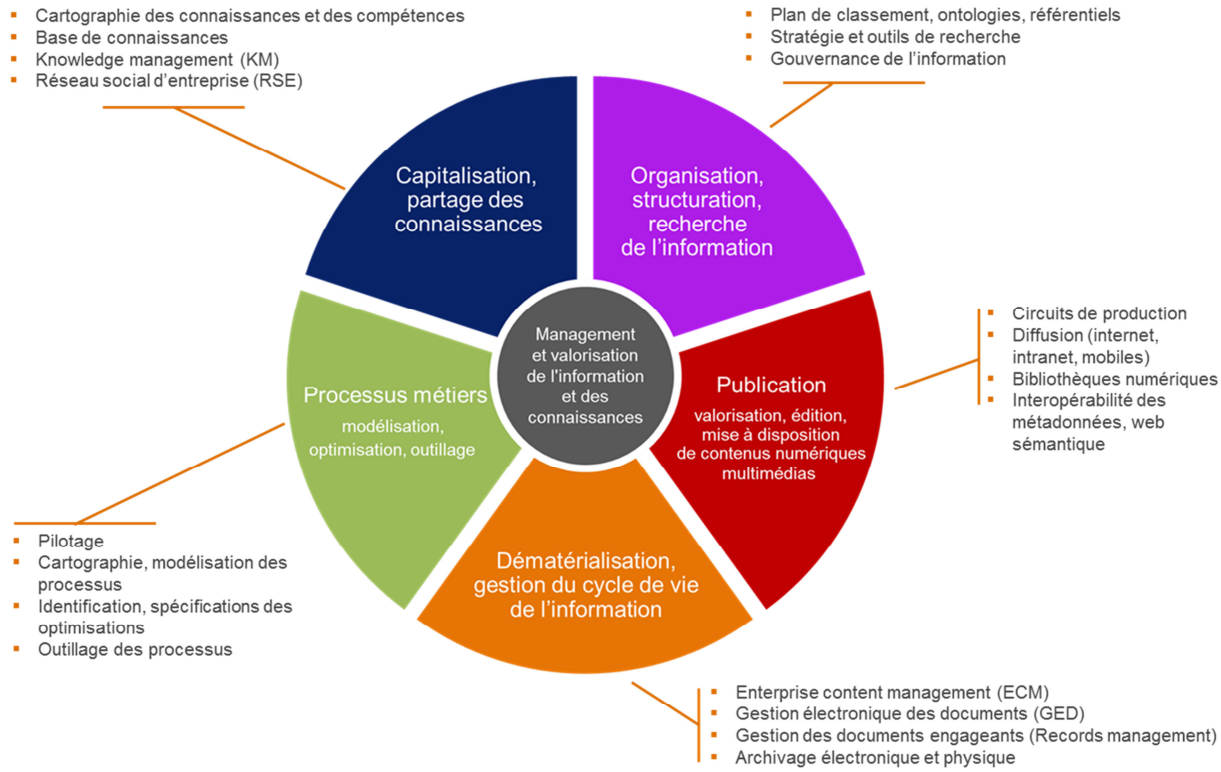
Trois mille ans avant notre ère, les marchands de la ville d'Ourouk se posaient déjà la question d'identifier des objets au moyen de signes durables et de communiquer ces données. Ils consignèrent ainsi, sur des tablettes d'argile, le premier système d'écriture.

PRESENTATION DU CABINET OUROUK

Créé en 1992, Ourouk est un cabinet de conseil en management et en valorisation de l'information et des connaissances. Le cabinet, indépendant depuis son origine, est constitué d'une équipe de 14 consultants. Son chiffre d'affaires connaît une progression moyenne depuis 2000 de 12 % par an. Dans toutes les organisations et dans chacun de leurs services, le management de l'information et des connaissances est devenu un enjeu clé pour :

- Partager et valoriser les données, les informations et les connaissances, qui constituent le patrimoine intellectuel de l'organisation,
- Accroître la performance marketing et commerciale,
- Stimuler l'innovation,
- Développer l'efficacité administrative et réduire les coûts,
- Garantir la mise en conformité réglementaire.

Nos domaines d'expertise



Nos consultants couvrent la totalité du cycle de vie d'un projet, du cadrage au déploiement.

Nous réalisons également des prestations de traitement de l'information et du document.

Nos clients sont situés dans le domaine de l'énergie, de la pharmacie, banque-assurance, collectivités territoriales, secteur public, édition et médias, secteur culturel…

tessi GED

DOCUBASE

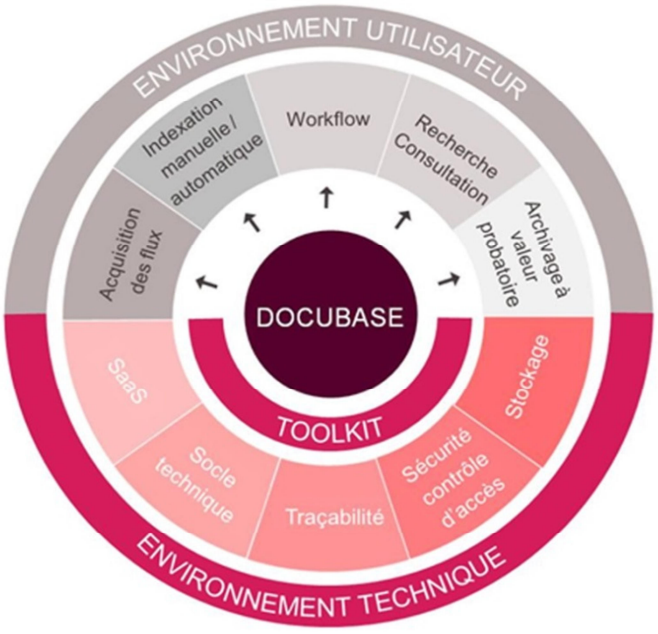
De la gestion de contenu à l'archivage électronique à valeur probatoire

Filiale du pôle d'activités Tessi documents services, Tessi GED est éditeur et intégrateur de solutions de gestion de contenu. Son offre de progiciels est le fruit de 20 années d'expérience acquise auprès de 2.000 clients installés.

La gamme DOCUBASE fournit et intègre l'ensemble des briques nécessaires à la mise en œuvre d'une solution complète de gestion du cycle de vie des documents et de l'information : capture des documents, gestion et collaboration autour des contenus, conservation et archivage électronique à valeur probatoire. Véritable élément au cœur du système d'information de l'entreprise, DOCUBASE s'intègre naturellement à la chaîne de traitement de l'information grâce à des services additionnels pour une intégration forte avec les applications métiers et les systèmes de gestion (ERP).

En complément de son système d'archivage électronique, DOCUBASE dispose nativement d'un dispositif logiciel de coffre-fort numérique, permettant de garantir la valeur probatoire des objets déposés.

La solution d'archivage électronique DOCUBASE est disponible soit en mode SaaS, internalisé au sein des entreprises, soit en mode SaaS.



Tessi GED
56 rue de Billancourt • 92100 Boulogne-Billancourt
Tél. +33 (0)1 55 18 00 18
sales.docubase@tessi.fr

La gestion de contenu au service de votre métier

EVER TEAM est le 1er éditeur européen de solutions intégrées de gestion de contenu d'entreprise ECM. Seul acteur français dans le « Magic Quadrant » des solutions ECM établi par le cabinet Gartner, EVER TEAM totalise plus de 20 années d'expertise et d'innovation dans le domaine de la gestion de contenu.

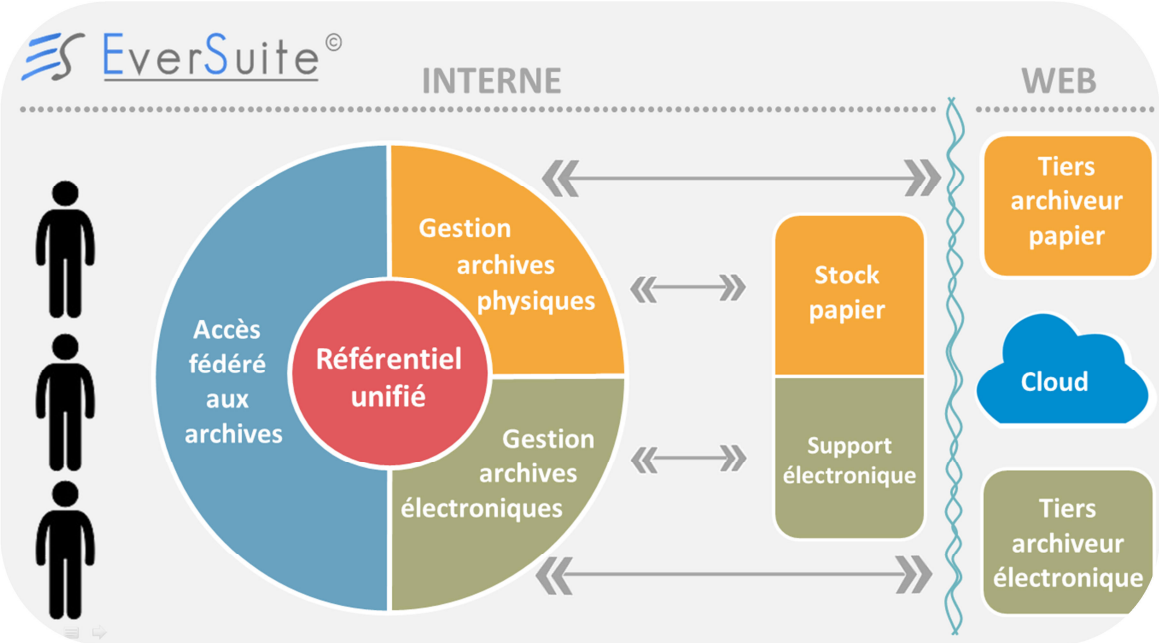
Les logiciels **EverSuite** constituent une suite modulaire et intégrée, permettant de résoudre les problématiques de gestion de contenu les plus fréquemment rencontrées : référentiel documentaire, gestion électronique de documents, workflow et automatisation des processus métier, conversation & archivage et conformité réglementaire, et valorisation de l'information.

EverSuite Compliance

Logiciel d'archivage mixte de documents électroniques et papier

EverSuite Compliance permet de mettre en œuvre d'un système d'archivage mixte sécurisé et évolutif. Il répond à vos besoins d'archivage quelle que soit la nature de l'archive : électronique (SAE), physique ou hybride au sein d'une même application. Respectant les normes archivistiques et les exigences légales de traçabilité et de conservation internationales, **EverSuite Compliance** préserve l'intégrité de l'information afin de garantir une vocation probatoire forte aux archives en cas de litige. C'est l'outil idéal en vue d'une certification NF 461.

EverSuite Compliance est disponible en mode internalisé au sein de votre entreprise ou en mode SaaS via nos partenaires.



EVER TEAM
17 Quai Joseph Guillet - 69004 LYON - France
336 Rue Saint-Honoré - 75001 PARIS - France
Tél. +33 (0)4 26 68 33 00

Cabinet d'études et de conseils spécialisé dans les domaines des systèmes de gestion électronique de documents (Bases documentaires ou GED) et archivage électronique sécurisé à valeur probatoire

Etudes préalables, cahier des charges, conseil, formation, assistance à maîtrise d'ouvrage, suivi de projet

Etude de marchés, assistance marketing.

Sirius Systems est membre du comité de normalisation CN171 de l'AFNOR et ISO TC 171, certifié CDIA+ par CompTIA (USA) et expert habilité auprès de l'AFNOR pour les audits de certification des systèmes d'archivage NF 461.

Membre APROGED.

Spécialités : stratégie d'archivage et gestion de documents dans le secteur Banque/Assurance et opérateurs télécom, mise en place de système d'archivage électronique sécurisé,
audit de conformité à la norme Z42-013.

Architecture de systèmes de confiance liés à la dématérialisation des échanges

Sirius Systems France
29 Avenue du Plateau
78990 Elancourt
Téléphone : 33 1 30 50 07 17
Télécopie : 33 1 30 50 07 17
Email : info@sirius-system.com

RSD, éditeur suisse de logiciels d'archivage depuis 1973, est aujourd'hui un acteur majeur de la Gouvernance de l'Information. Conscient des enjeux que représente le capital informationnel des entreprises, RSD leur permet de contrôler et de gérer le cycle de vie de leurs documents engageants (records), quel que soit le pays, la politique de conservation ou la réglementation applicable. Les solutions innovantes de RSD sont utilisées par des millions d'utilisateurs et répondent aux besoins de nombreuses entreprises souhaitant réduire leurs coûts d'exploitation et leur exposition aux risques. RSD est présent en Europe à Genève, Zurich, Londres, Paris et Madrid, en Amérique du Nord à Boston et New York, et s'appuie aussi sur son réseau mondial de partenaires pour satisfaire aux exigences de ses clients. RSD est aussi un membre actif des principales associations professionnelles européennes et internationales (ARMA, Aproged, FedISA).

Notre Vision :

La gouvernance de l'information est un nouveau défi. La croissance du nombre de documents, et autres contenus, créés ou reçus par les entreprises est exponentielle. Parallèlement, les exigences réglementaires sont de plus en plus strictes notamment pour ce qui relève de l'audit, du suivi, de la conservation et de la mise à disposition de l'information, d'où la nécessité pour les entreprises de retrouver rapidement les documents et les contenus recherchés.
Le défi de la gouvernance de l'information – les règles et les processus de l'entreprise assurant une gestion efficace de l'information, en totale conformité avec les exigences réglementaires en vigueur – dépasse de loin les défis combinés de la gestion documentaire, du « records management », de l'archivage, de la restitution de documents et de la gestion du contenu.

Notre Offre : RSD GLASS

RSD GLASS est une solution utilisée pour mettre en place un programme global de gouvernance de l'information pour tous types de documents engageants (électroniques et papier). Avec RSD GLASS, les entreprises créent leurs politiques de gestion des documents sensibles, et les appliquent de manière proactive à travers toute l'organisation, les systèmes informatiques, les entrepôts de contenu et les archives physiques, quelle que soit leur entité géographique. Les utilisateurs de RSD GLASS peuvent décider des informations qu'ils souhaitent conserver et supprimer telles que les informations ne présentant plus de nécessité, leur cycle de vie ayant atteint leur terme. Ceci leur permet de réduire à la fois le volume et les coûts de stockage. L'autre atout réside dans la réduction des frais juridiques en cas de litiges et la moindre exposition au risque informationnel. RSD GLASS permet de gérer de façon centralisée et proactive les différences juridictionnelles des autres pays où l'entreprise est présente.

Une ouverture vers le Cloud :

Comme les informations des entreprises peuvent se trouver dans un environnement cloud ou hors cloud, RSD GLASS offre la souplesse d'un déploiement SaaS ou sur site, ou mixte appelé hybride.
Chaque entreprise en fonction du niveau de sensibilité de l'information décidera de placer son contenu dans l'environnement le plus adapté (Sur ses sites (On Premise), dans le Cloud ou de manière hybride.)
tout en maintenant une gouvernance centrale mais applicable pour chaque environnement.

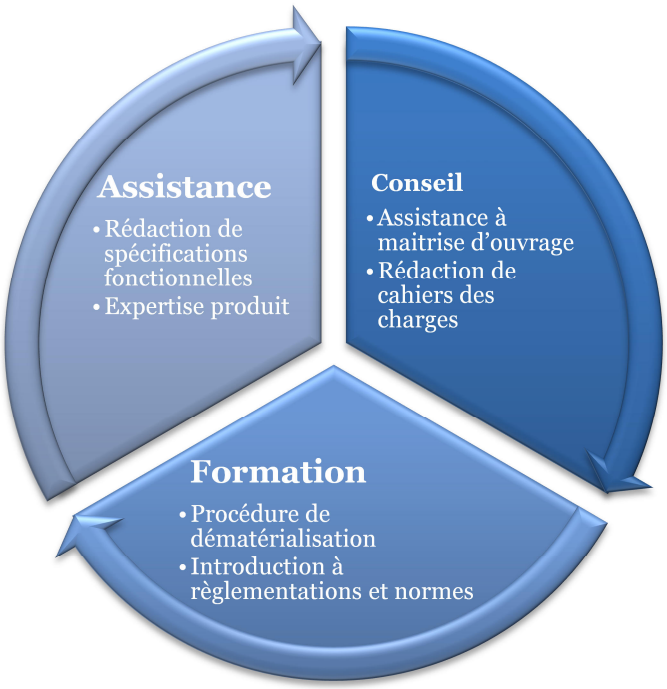
Coté respect des normes NFZ et en particulier NFZ 42-013, RSD GLASS Repository le module de coffre-fort électronique de RSD GLASS , rempli tous les prérequis techniques nécessaires afin qu'une organisation puisse passer avec succès sa possible certification NF461. Et permet ainsi à l'entreprise de s'assurer de la conservation et l'intégrité des documents stockés dans ces systèmes.

PRESENTATION DE DOC@WORK

doc@work est un **cabinet de conseil**, spécialisé dans la **gestion des documents électroniques**. Son expertise est le résultat de 10 ans de travail dans la mise en place de systèmes de **dématérialisation**, **d'archivage** et de **signature électronique**. doc@work vous accompagne dans la mise en place ou l'externalisation de services qui assurent le cycle de vie du document, qu'il soit un original électronique ou un document numérisé.

Face à l'émergence des services « Cloud », doc@work vous propose ses services pour vous permettre de sortir du brouillard généré par la multitude d'offres et réglementations.

Lorsque le buzz du moment est « Big Data », doc@work apporte une approche holistique du flux documentaire, pour minimiser la quantité de données sauvegardées et maximiser la valeur ajoutée obtenue par l'analyse de cette masse d'informations.



Domaines d'intervention

- Conseil pour la conduite de projet de gestion documentaire (dématérialisation, gestion des flux, archivage, archivage à valeur probatoire), réglementé ou pas.
- Conseil pour le choix d'un sous-traitant pour externaliser la gestion des flux documentaires.
- Optimisation de processus et flux documentaires.
- Support à l'utilisation et à la configuration de services et progiciels.
- Formations.

Compétences

- Assistance à maitrise d'ouvrage.
- Rédaction d'expression de besoin et cahier des charges.
- Conception de solutions, rédaction des spécifications fonctionnelles.
- Analyse des propositions, aide au choix du sous-traitant.
- Expertise produits : conseil sur le choix de progiciels, calibrage et paramétrage de progiciels.