Politique d'Archivage

Service d'Archivage Electronique Sécurisé de Données Numériques

Nom : Politique d'Archivage – Service d'Archivage Electronique Sécurisé de Données Numériques
Référence : D-PM-10.2_PA
Version : 1.3.11
Date : 26.11.2024
Date d'application : 26.11.2024
Diffusion : PUBLIQUE

Docaposte Arkhineo, une société de Docaposte
Siège social : 45/47 boulevard Paul Vaillant Couturier - 94200 Ivry-sur-Seine
SAS au capital de 100 000 € - 435 405 923 RCS CRÉTEIL - Siret 435 405 923 00069 - TVA Intracommunautaire FR 67 435 405 923
Bureaux : 24 rue Drouot - 75009 Paris - Tél. : 01 78 09 39 10

Historique des modifications

Date	Version	Intervenant	Objet	Statut
Historique antérieur tronqué.				
2016-01-15	1.3.6	NRo	Plan de secours Informatique : reprise de données sans perte ; Application de la Z42-013 au niveau renforcé ; Migration de format ; Précision sur le risque que constitue l'emploi de formats non préconisés à l'égard de la pérennité des documents archivés ; Précision sur la restitution du cycle de vie ; Ajout de la prorogation/abrégement ; Emploi de la terminologie "copie de sauvegarde" plutôt que "copie de sécurité" ; Redécoupage de la présentation des journaux.	Diffusable
2017-05-05	1.3.7	PDe	Mise à jour des textes juridiques applicables.	Diffusable
2021-05-07	1.3.8	NRo	Précisions relatives à la déclaration des pratiques de validation et de conservation des signatures et cachets électroniques qualifiés. Mise à jour charte graphique.	Diffusable
2021-05-07	1.3.9	NRo	Précisions relatives à la localisation des sites de conservation et de sauvegarde.	Diffusable
2023-11-28	1.3.10	NRo VL	Passage de diffusion RESTREINTE à diffusion PUBLIQUE. Troncature de l'historique antérieur à 2016. Précision sur les parties prenantes. §6.2 Parties prenantes §5 DICT	Diffusable
2024-11-26	1.3.11	VL	§5.1.10, §6.2 §7.2.3.1 §7.2.3.2 Changement des DataCenters Data4+Equinix+CDC-EDF-Val-deReuil	Diffusable

Arkhineo

Sommaire

1 Introduction 7
1.1 Présentation générale de la politique d'archivage 7
1.2 Objet de la politique d'archivage 7
1.3 Champ d'application de la politique d'archivage 7
1.4 Identification de la politique d'archivage 7
2 Définitions 8
3 Contexte Juridique 10
3.1 La preuve des actes juridiques 10
3.2 L'intégrité de l'écrit électronique 10
3.3 La validité des actes juridiques 10
3.4 Textes Juridiques applicables 11
3.4.1 Cadre Communautaire 11
3.4.2 Cadre français 11
3.4.3 Spécificités du Secteur publique 12
4 Normes applicables et valeur de celles-ci 13
5 Principes fonctionnels 14
5.1 Versement ou Capture 15
5.1.1 Contrôle de l'origine et de la destination du versement 16
5.1.2 Objet d'archives et métadonnées 16
5.1.3 Indexation 16
5.1.4 Validation de l'Objet d'Archives 16
5.1.5 Identifiant Unique d'Archive 17
5.1.6 Horodatage 17
5.1.7 La sécurisation de l'Archive 17
5.1.8 Scellement numérique 17
5.1.9 La preuve de dépôt 18
5.1.9.1 L'acquittement technique (AT) 18
5.1.9.2 L'accusé de réception fonctionnel (ARF) 18
5.1.10 Copie de sauvegarde 18

5.2 Consultation 18
5.2.1 Recherche multicritères 19
5.2.2 Accès à l'archive 19
5.2.3 Communication (ou extraction) en nombre 19
5.2.4 Certificat de conformité à l'original 20
5.3 Réversibilité 20
5.3.1.1 Restitution 20
5.3.1.2 Communication 20
5.4 Fin de vie 20
5.4.1 Durée de service 20
5.4.2 Durée de conservation 21
5.4.3 Consultation au-delà de la durée de service 21
5.4.4 Restitution, destruction ou prorogation en fin de période de conservation 21
5.4.4.1 Cas particulier des clients du client 21
5.4.4.2 Cas particulier des archives publiques 22
5.5 Modification d'archive 22
5.6 Destruction d'archive 22
5.7 Gel et dégel d'archives 23
5.8 Prorogation/abrégement 23
6 Principes Organisationnels 24
6.1 Les engagements du Tiers-archiveur 24
6.2 Conservation intègre sur la durée convenue 24
6.2.1 Disponibilité de la plateforme 25
6.2.1.1 Haute disponibilité 25
6.2.1.2 Performance 25
6.2.1.3 Support client 25
6.2.2 Sécurité 25
6.2.2.1 Intégrité 26
6.2.2.2 Pérennité 26
6.2.2.3 Confidentialité 26
6.2.2.4 Traçabilité 27
6.2.3 Réversibilité 28
6.2.4 Validation et conservation des signatures et cachets électroniques qualifiés 28
6.3 La responsabilité du client 29
6.3.1 Politique d'Archivage 29
6.3.2 Format des données 29
6.3.3 Versement 30
6.3.4 Vérification des Accusés de réception 30
6.3.5 Vérification des signatures 30
7 Principes de mise en œuvre 31
7.1 Échanges entre le Tiers Archiveur et le client 31

7.2 La sécurité 31
7.2.1 Politique de Sécurité de l'Information (PSI) et Plan de Continuité d'Activité (PCA) 31
7.2.2 Développement logiciel 31
7.2.3 Sécurité physique et environnementale 32
7.2.3.1 Deux sites actifs 32
7.2.3.2 Site de sauvegarde 32
7.2.4 Contrôle d'accès 32
7.2.5 Sécurité des matériels 32
7.2.6 Sécurité des logiciels 33
7.2.7 Sécurité des systèmes d'information 33
7.2.8 Sécurité liée aux ressources humaines 33
8 Principes techniques 34
8.1 Horodatage 34
8.2 Scellement 34
8.3 Disques réinscriptibles avec moyens cryptographiques 34

Avertissement

1 INTRODUCTION

1.1 Présentation générale de la politique d'archivage

Ce document constitue la Politique d'Archivage de la société Docaposte Arkhineo agissant en tant qu'Opérateur de Système d'Archivage (ci-après désigné « Tiers Archiveur ») pour les besoins de ses clients ayant souscrit au Service d'Archivage Electronique Sécurisé de Données Numériques de la Société appelé Arkhineo.

Ce document définit les engagements standards du Tiers Archiveur. Il ne se substitue pas à la Politique d'Archivage du client. Le client ayant souscrit au Service SAE de Docaposte Arkhineo est encouragé à définir sa propre politique d'archivage compatible avec la Politique d'Archivage, objet de ce document.

Cette Politique d'Archivage ne peut se substituer au contrat ADE et ses Annexes qui régissent les relations contractuelles entre le client et la Société.

La Politique d'Archivage est maintenue à jour par la société afin de refléter les évolutions du service.

1.2 Objet de la politique d'archivage

La présente Politique d'Archivage a pour objet de conserver la valeur juridique initiale de l'écrit sous forme électronique pendant toute sa durée de conservation.

1.3 Champ d'application de la politique d'archivage

Le champ d'application de la présente Politique d'Archivage s'étend a priori à l'ensemble des actes établis par voie électronique lorsque les textes le permettent, qu'il s'agisse de documents relevant du droit privé comme du droit public et qui ont été transmis au Coffre-fort électronique®.

1.4 Identification de la politique d'archivage

La présente politique d'archivage, désignée sous le nom de ***Politique d'Archivage - Service d'Archivage Electronique Sécurisé de Données Numériques,*** est référencée par l'OID 1.3.6.1.4.1.29371.1.1.3.2

2 DEFINITIONS

Accusé de Réception Fonctionnel (ARF) : certificat de dépôt d'un Objet d'archives, retourné au client. Il comporte l'IUA, l'empreinte de l'Objet d'archives, l'horodatage du dépôt et les métadonnées nécessaires à son identification. La réception d'un ARF mentionnant une archive atteste la bonne prise en compte de l'archive et marque le début des engagements de Docaposte Arkhineo concernant cette archive.

Archive : ensemble composé de l'Objet d'archives et des métadonnées associées reçu, conservé et communiqué par le Système d'Archivage Electronique de Données Numériques.

Coffre-fort (Coffre) : espace d'archivage attribué par le Tiers-archiveur à un client.

Communication : ensemble des mécanismes permettant de rechercher et de communiquer des documents numériques à des fins de gestion, de preuve ou patrimoniales.

Contrat ADE (Contrat) : Contrat d'Archivage désigné par **«** Contrat d'Archivage de Données Electroniques » souscrit par le client auprès de la Société.

Document Electronique : synonyme d'Objet d'archives.

Données Numériques : un train de bits représentant une information soit nativement numérique soit provenant d'une numérisation (dématérialisation).

Empreinte : ensemble de bits caractéristique d'un document numérique. L'empreinte est obtenue par l'application d'une fonction de hachage. Toute modification du document entraînera une empreinte différente qui révélera la modification par comparaison avec la première empreinte.

Espace client : Espace sécurisé dédié au client contenant toutes les informations, références, identifiants nécessaires à la gestion du compte du client et aux espaces d'archivage (Coffre, Section, Compartiments ...) qui lui sont associés.

Horodatage d'une donnée : Information permettant de prouver qu'une donnée existait à un instant donné.

Identifiant Unique d'Archive (IUA) : Référence unique et permanente attribuée à un Objet d'archives par le SAE au moment du dépôt.

Métadonnées : ensemble structuré d'informations techniques, de gestion et de description attaché à un document servant à décrire les caractéristiques de ce document en vue de faciliter son repérage, sa gestion, sa consultation, son usage ou sa préservation.

Objet d'archives : Données (par exemple : contrat, facture, fiche de paye etc.) qui font l'objet de l'archivage (définition issue du Standard d'échange de données pour l'archivage – Direction Générale de la Modernisation de l'Etat et Direction des Archives de France)

Plan de Continuité d'Activité (PCA) : Ensemble de mesures visant à assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise puis la reprise planifiée des activités.

Plan de Secours Informatique : Sous-ensemble du PCA qui couvre les moyens informatiques. Il garantit la reprise des systèmes désignés comme critiques dans le temps minimum fixé. Il garantit également la reprise des données sans perte.

Politique d'archivage (PA) : ensemble de règles portant un nom qui indique les exigences relatives à un archivage électronique sécurisé pour une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes.

Politique de Sécurité de l'Information (PSI) : document, validé par la Direction Générale, décrivant le cadre dans lequel la démarche de sécurité de l'information s'inscrit.

Restitution : Ensemble des mécanismes permettant de rechercher et de remettre les documents numériques à l'organisme qui les a produits ou à ses mandants, puis de les détruire au sein de son système d'archivage.

Scellement numérique : Procédé permettant de garantir l'intégrité du document par l'utilisation conjointe de fonctions de hachage de signature numérique et optionnellement d'horodatage.

Section de coffre : L'ensemble des sections d'un Coffre constitue une partition d'un Coffre. Chaque section possède sa propre définition des métadonnées, sa propre durée de conservation. Une section permet de regrouper au sein d'un Coffre d'un client des documents d'un même profil d'archivage (durée de conservation et métadonnées identiques).

Service d'Archivage Electronique Sécurisé de Données Numériques (SAE) : Système d'Archivage Electronique destiné à traiter des Archives constituées uniquement de Données Numériques.

***SLA – Service Level Agreement* – Contrat de Niveau de Service :** la partie du contrat de service dans lequel on formalise la qualité du service.

Société : désigne Docaposte Arkhineo.

Système d'Archivage Electronique : système consistant à recevoir, conserver, traiter, restituer des Archives et qui s'appuie sur une plate-forme informatique**.**

Tiers Archiveur : Personne morale opérant un Service d'Archivage Electronique Sécurisé de Données Numériques (en charge de recevoir, conserver et restituer les Archives) pour le compte de ses clients.

Versement : transmission par un client d'un document numérique au SAE.

3 CONTEXTE JURIDIQUE

3.1 La preuve des actes juridiques

La loi n°2000-230 du 13 mars 2000, en rendant la preuve littérale indépendante de son support, a considérablement élargi le champ d'admission de la preuve.

Depuis cette loi n°2000-230 du 13 mars 2000 (J.O. du 14 mars 2000, p. 1968), l'écrit sous forme électronique est intégré dans le dispositif probatoire et notamment dans le système légal de la preuve.

En matière électronique, conformément à l'article 1316-1 du Code civil, pour valoir en justice, un écrit sous forme électronique doit permettre que « puisse être dûment identifiée la personne dont il émane et qu'il soit établi et **conservé dans des conditions de nature à en garantir l'intégrité** ».

Le respect des exigences du code civil et du décret d'application n°2001-272 du 30 mars 2001 relatif à la signature électronique, permet à l'écrit sous forme électronique de constituer une preuve parfaite ne pouvant être qu'incidemment remis en cause devant le juge.

A défaut, l'écrit sous forme électronique ne constituera alors qu'un élément de preuve parmi d'autres conformément aux dispositions du Code civil.

Dans ce cas, pour emporter la conviction du juge, il faudra établir la fiabilité du procédé utilisé et archiver les éléments de preuve pour les matières où la preuve contractuelle est libre. Il convient donc de s'appuyer sur le niveau de sécurité le plus élevé.

3.2 L'intégrité de l'écrit électronique

Conformément à cet article 1316-1 du Code civil, l'écrit sous forme électronique doit être « établi et conservé dans des conditions de nature à en garantir l'intégrité ». Cette intégrité de l'écrit sous forme électronique doit donc être garantie de son établissement jusqu'au terme de la durée de conservation et ce, afin qu'il soit recevable en tant que preuve au même titre que l'écrit sur support papier.

L'écrit archivé ne doit donc avoir subi aucune altération ni modification.

Il est recommandé de conserver l'écrit, la signature électronique et les éléments qui sont associés (certificat, liste de certificats révoqués etc...) afin de pouvoir ultérieurement vérifier la signature électronique.

3.3 La validité des actes juridiques

L'article 1108-1 du Code civil prévoit que les actes juridiques indispensables à la validité (crédit à la consommation, crédit immobilier, statuts de société,...), à l'exception de ceux indiqués à l'article 1108-02 relatifs notamment au droit de la famille, peuvent être établis et conservés sous forme électronique si les articles 1316-1 et 1316-4 du Code civil sont respectés.

En l'absence d'écrit, la valeur juridique de ces actes pourrait être remise en cause.

3.4 Textes Juridiques applicables

3.4.1 Cadre Communautaire

- Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique ») (J.O.C.E., n° L 178 du 17 juillet 2000, p. 1 et s.) ;
- Directive 2002/65/CE du Parlement européen et du Conseil du 23 septembre 2002 concernant la commercialisation à distance de services financiers auprès des consommateurs et modifiant les directives 90/619/CEE du Conseil, 97/7/CE et 98/27/CE (J.O.C.E. n° L. 271 du 9 octobre 2002, p. 17 et s) ;
- Directive n° 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, modifiant la directive n°2002/58/CE, (J.O.U.E. L 105 du 13 avril 2006, p. 54. Directive dite « du premier pilier ») ;
- Directive 2006/112/CE du Conseil du 28 novembre 2006 relative au système commun de taxe sur la valeur ajoutée (*J.O.U.E. L 347 du 11 décembre 2006, p. 1 et s) ;*
- Directive 2007/64/CE du Parlement européen et du Conseil du 13 novembre 2007 concernant les services de paiement dans le marché intérieur, modifiant les directives 97/7/CE, 2002/65/CE, 2005/60/CE ainsi que 2006/48/CE et abrogeant la directive 97/5/CE (Texte présentant de l'intérêt pour l'EEE) (J.O.U.E L 319 du 5.12.2007, p. 1 et s) ;

3.4.2 Cadre français

- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (J.O. du 14 mars 2000, p. 3968) ;
- Loi n°2002-1576 du 30 décembre 2002 de finances rectificatives pour 2002 (J.O. du 31 décembre 2002, p. 22070 et s.) ;
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (J.O. du 22 juin 2004, p. 11168 et s.) ;
- Ordonnance n°2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique (J.O. du 17 juin 2005, p.10342) ;
- Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique (J.O. du 31 mars 2001, p. 5070) ;
- Décret n° 2003-632 du 7 juillet 2003 relatif aux obligations de facturation en matière de taxe sur la valeur ajoutée et modifiant l'annexe II du code général des impôts et la deuxième partie du livre des procédures fiscales (J.O. du 9 juillet 2003, p. 11617 et s.).
- Décret n° 2003-659 du 18 juillet 2003 relatif aux obligations de facturation en matière de taxe sur la valeur ajoutée et modifiant l'annexe III du code général des impôts et la deuxième partie du livre des procédures fiscales (J.O. du 20 juillet 2003, p. 12272 et s.).
- Décret n° 2005-137 du 16 février 2005 pris pour l'application de l'article L. 134-2 du code de la consommation (J.O. du 18 février 2005, page 2780) ;
- Instruction fiscale de la Direction Générale des Impôts du 7 août 2003 – Taxe sur la valeur ajoutée. Obligations des assujettis. Obligations relatives à l'établissement des factures (Bulletin officiel des impôts, n° spécial, 3 C.A., n° 136 du 7 août 2003) ;
- Instruction fiscale de la Direction Générale des Impôts du 24 janvier 2006 sur les contrôles de comptabilités informatisées (Bulletin officiel des impôts, n°12 13 L-1-06 du 24 janvier 2006) ;

- Instruction fiscale de la Direction Générale des Impôts du 11 janvier 2007 sur les obligations relatives à la conservation des factures – mesure d'assouplissement (Bulletin officiel des impôts, n°4, 3 E-1-07 du 11 janvier 2007) ;

3.4.3 Spécificités du Secteur publique

Définition des archives publiques :

> Article L.211-1 du code du patrimoine: « Les archives [publiques] sont l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité. »

Textes applicables :

- Ordonnance n° 2004-178 du 20 février 2004 relative à la partie législative du code du patrimoine abroge la loi n°79-18 du 3 janvier 1979 relative aux archives publiques ou privées ;
- Code des marchés publics issu du décret n°2006-975 du 1er août 2006 portant code des marchés publics, (J.O. du 4 août 2006) ;
- Loi n°2008-696 du 15 juillet 2008 relative aux archives modifie le code du patrimoine et introduit (article L 212-4-II du code du patrimoine) la possibilité pour les archives publiques durant leur âge intermédiaire d'être confiées à des tiers agréés à cette fin par le Ministère de la Culture, à condition qu'elles soient éliminables à terme (cf article L212-4, § III).;
- Décret n° 2011-573 du 24 mai 2011 relatif à la partie réglementaire du code du patrimoine 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.
- Standard d'Echange de Données pour l'Archivage (SEDA) qui modélise les différentes interactions qui peuvent avoir lieu entre des acteurs dans le cadre de l'archivage de données. Ces interactions sont au nombre de six : le transfert, la demande de transfert, la modification, l'élimination, la communication et la restitution. Les acteurs sont au nombre de cinq : le service producteur, le service versant, le service d'archives, le service de contrôle et le demandeur d'archives.
- Décret n°79-1037 du 3 décembre 1979 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.

4 NORMES APPLICABLES ET VALEUR DE CELLES-CI

Une norme technique se définit comme une « spécification technique approuvée par un organisme reconnu à activité normative pour application répétée ou continue, dont l'observation n'est pas obligatoire » (Directive 83/189/CEE mod. du Conseil du 28 mars 1983).

Bien que les normes ne constituent que des recommandations techniques sans force obligatoire, elles sont généralement considérées comme codification écrite regroupant « les règles de l'art ».

La Cour de cassation a d'ailleurs confirmé cette conception en considérant que l'existence d'une norme permet de représenter l'état de l'art dans le domaine auquel elle se rapporte (Cass. civ. 3ème, 4 février 1976, Bull. civ. III, n°49).

La conception et l'exploitation d'un système d'archivage électronique répondent à la norme AFNOR NF Z 42-013.

Cette norme NF Z 42-013 a été traduite en anglais et a donné naissance à la norme ISO_14641-1.

Docaposte Arkhineo, par la conception et l'exploitation de son Système d'Archivage Electronique Sécurisé de Données Numériques, applique la norme Z42-013 au niveau de sécurisation « renforcé ».

5 PRINCIPES FONCTIONNELS

Le Tiers Archiveur propose un Service d'Archivage Electronique Sécurisé de Données Numériques. Il s'engage, auprès de ses clients ayant souscrit au service, à :

- Accepter des Objets d'Archives en sécurisant le versement des Documents Electroniques,
- Conserver ces documents dans des conditions de nature à garantir la **Disponibilité**, l'**intégrité**, la **Confidentialité** et la **Traçabilité / Preuve** de ces documents (critères de sécurité DICT, DICP) pendant toute la durée de conservation prévue,
- Permettre la consultation en ligne des Archives aux personnes autorisées
- À la fin de la période de conservation, demander au client s'il convient de :
  - proroger la durée de conservation ;
  - restituer les archives ;
  - détruire les archives.

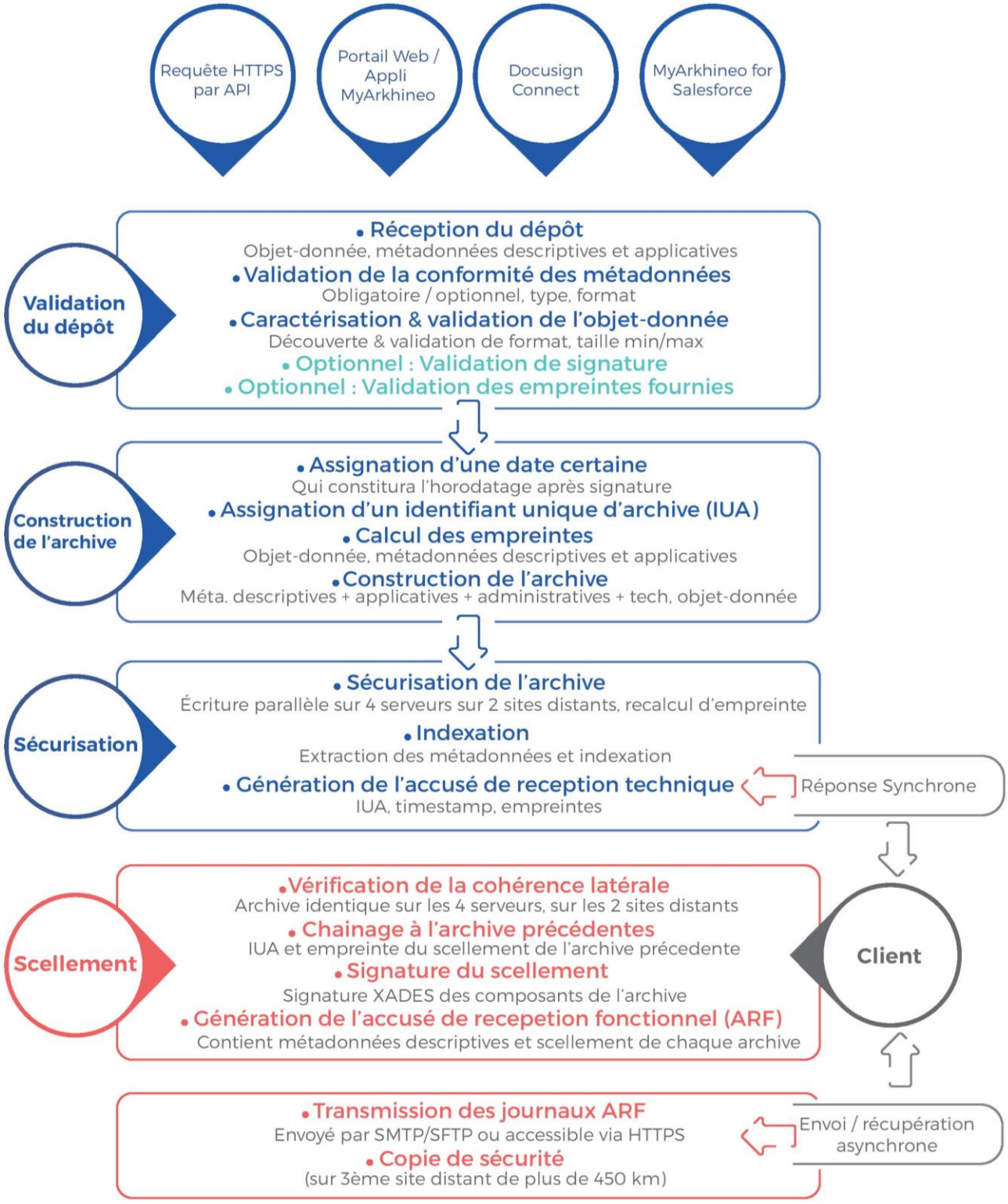
Ce chapitre décrit les principes fonctionnels qui sous-tendent le Service d'Archivage Electronique Sécurisé de Docaposte Arkhineo.

La fonction d'archivage de documents électroniques consiste à conserver, puis restituer à la demande ces documents pendant une période prédéfinie, dans le respect et la garantie de l'intégrité numérique des données initialement déposées, tel que défini dans le texte de loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et du Code Civil modifié en conséquence.

Le système tiers d'archivage ne crée pas la valeur probante, ou la valeur légale, des documents qui y sont déposés puis conservés. Celle-ci est inhérente au procédé source applicatif ou métier qui « fabrique et formate » en amont les documents de façon telle que cette dimension probante ou légale y soit rattachée dès son origine.

En revanche, le système tiers d'archivage maintient la valeur probante (ou probatoire) des documents déposés pendant toute la durée de conservation convenue.

5.1 Versement ou Capture



5.1.1 Contrôle de l'origine et de la destination du versement

Le Tiers-archiveur contrôle la provenance du flux capturé. Le versement doit provenir d'un client référencé et être à destination d'un Coffre-fort autorisé pour ce client.

L'acheminement des données à archiver doit utiliser des moyens de communication sécurisés garantissant l'authentification des interlocuteurs et la confidentialité des données.

5.1.2 Objet d'archives et métadonnées

L'ensemble logique de Données Numériques (objet d'archives) transmise par le client, objet du versement, destiné à être conservé par le Tiers-archiveur doit être accompagné des métadonnées nécessaires à sa gestion dans le temps.

Outre les **métadonnées administratives** nécessaires à l'identification du client, de la Politique d'Archivage concernée (durée de conservation…) et du Coffre-fort de destination, les **métadonnées descriptives** (auteur, titre, date, format …) et **les métadonnées applicatives** (liées au métier du client) peuvent accompagner l'Objet d'archives pour permettre son indexation et donc sa consultation ultérieure.

5.1.3 Indexation

L'indexation est réalisée lors du dépôt de l'archive, les métadonnées indexées permettant de retrouver efficacement une archive (cf. § 5.2.1). Seul le bon déroulement de cette indexation, qui vérifie la présence des métadonnées et leur format, permet de sécuriser l'archive. Dans le cas contraire l'archive est rejetée.

5.1.4 Validation de l'Objet d'Archives

Le Tiers Archiveur préconise l'emploi par le Client de formats de fichiers standards, normalisés et pérennes. Ces formats sont précisés dans le document de référence E-MA-20_LISTE-FORMATS, et le client est invité à choisir un ou plusieurs formats parmi cette liste.

Lors du dépôt, le Tiers-Archiveur procède à la validation de l'Objet d'archive au regard du ou des formats choisis, et tout Document Electronique ne satisfaisant pas le format, ou l'un des formats choisis est rejeté.

Le Tiers Archiveur ne procède en aucun cas à une quelconque analyse sémantique du contenu de l'Objet d'archive. Seul le format du fichier est contrôlé et validé : la conformité de la structure du fichier au regard des spécifications du format.

L'emploi des formats préconisés garantit la pérennité des documents archivés, et permet à Docaposte Arkhineo d'effectuer les migrations de formats en cas d'obsolescence.

Si le Client choisit de chiffrer ses données, le Tiers Archiveur l'informe qu'il ne pourra valider le format des documents reçus. Enfin, le Client est informé que s'il choisit expressément de déposer ses Documents Electroniques dans un format non préconisé par le Tiers Archiveur, ce dernier ne sera pas en mesure de contrôler le format des fichiers entrants, bien qu'il soit en mesure de les conserver dans leur format d'origine.

Dans ce cas, le client reconnait être informé du risque que constitue l'emploi de formats non préconisés, quant à la pérennité des documents archivés ; Docaposte Arkhineo n'étant pas en mesure d'effectuer, en cas d'obsolescence, la migration de formats non préconisés.

5.1.5 Identifiant Unique d'Archive

Au moment du Versement (aussi appelé dépôt) d'un objet d'archives, un Identifiant Unique d'Archive (IUA) est attribué. La validité de cet IUA est garantie pendant toute la durée de conservation de l'archive.

L'IUA permet donc pendant toute la durée de conservation un accès direct à l'archive.

5.1.6 Horodatage

La date et l'heure certaines de constitution de l'archive dans le SAE sont enregistrées et scellées avec l'Objet d'archives au sein même de l'Archive.

Cette date et heure certaines sont fournies par un service de temps normalisé, s'appuyant sur plusieurs sources de temps (satellite, terrestre, etc.).

5.1.7 La sécurisation de l'Archive

Dès sa réception, après les contrôles sur les métadonnées et l'Objet d'archive, l'archive est sécurisée par écriture en parallèle sur 4 supports distincts répartis sur 2 sites indépendants.

Un acquittement technique (AT) (cf. § 5.1.9), garantissant la transmission et la sécurisation de l'archive est généré et retourné au client.

Dans un second temps, une copie de sécurité est réalisée sur le site de sauvegarde (cf. § 5.1.10).

Il existe donc en tout 5 copies de l'archive.

5.1.8 Scellement numérique

Le scellement numérique est un procédé cryptographique permettant de garantir l'intégrité de l'objet d'archives et des métadonnées pendant toute la durée de conservation.

Il comporte, en particulier, l'IUA, l'horodatage, les empreintes de l'objet d'archives, des métadonnées applicatives et des métadonnées descriptives.

Il comporte également le chaînage avec l'archive précédente permettant de constituer une chaîne ininterrompue d'archives dans laquelle il est impossible d'enlever, d'ajouter ou de substituer une archive sans altérer la chaîne.

Le calcul de l'empreinte de référence est réalisé par l'application d'une fonction de hachage cryptographique.

Le scellement de l'archive, incluant la date et l'heure, constitue une contremarque de temps établissant ainsi la preuve, par un tiers, que la donnée existait à cet instant-là.

Le scellement est systématiquement signé.

5.1.9 La preuve de dépôt

5.1.9.1 L'acquittement technique (AT)

Un acquittement technique est généré après validation des métadonnées et de l'Objet d'archive, lorsque l'archive est sécurisée c'est-à-dire dès qu'elle a été correctement enregistrée et indexée, en parallèle, sur 4 supports distincts répartis sur 2 sites différents.

L'AT comporte les empreintes de référence calculées, l'horodatage du dépôt ainsi que l'IUA attribué par le Service d'Archivage.

5.1.9.2 L'accusé de réception fonctionnel (ARF)

Dans un second temps, le processus asynchrones de scellement numérique de l'archive est réalisé. L'archive devient alors complètement fonctionnelle.

Un accusé de réception fonctionnel est alors constitué pour chaque archive, il comprend :

- les métadonnées permettant d'identifier l'archive ;
- le scellement, composé de :
  - l'Identifiant Unique de l'archive ;
  - les empreintes calculées ;
  - l'horodatage, le chaînage, la signature.

Un journal des ARF est mis à la disposition du client à une périodicité fixe (quotidiennement par exemple).

Le déposant dispose alors, d'une manière opposable, pour chaque archive, de la preuve du dépôt.

5.1.10 Copie de sauvegarde

D'une manière asynchrone, une copie de sauvegarde de l'archive est réalisée sur un site de sauvegarde distant de plus de 100 Km des deux sites principaux Actif/Actif.

5.2 Consultation

Les documents archivés sont accessibles en ligne aux personnes autorisées 24h sur 24h et 7 jours sur 7 Celles-ci pouvant être des tiers, autorisés par le client, intervenant ponctuellement dans le cadre d'une mission (contrôleurs fiscaux, auditeurs ...) ou les propres clients du client.

Le service de consultation est utilisable soit par l'intermédiaire de pages HTML, conçues pour être interactives, soit par l'intermédiaire d'une Web API RestFul (ou *Web Service)* directement intégrable dans les applicatifs du client. Ces deux modes de consultations s'effectuent selon les mêmes principes.

Le processus de consultation s'effectue en deux étapes :

- Recherche multicritères
- Accès à l'archive

5.2.1 Recherche multicritères

Après authentification, le système limite l'accès au seul Coffre-fort autorisé.

La première étape consiste alors à fournir des critères de sélection. Ceux-ci peuvent associer un intervalle de date de dépôt et des valeurs de métadonnées parmi celles pour la section de coffre correspondante.

En réponse, le système fournit, si la requête est pertinente, la liste des archives répondant à ces critères.

L'étape suivante consiste à sélectionner une référence et accéder à l'archive correspondante.

5.2.2 Accès à l'archive

À partir de la liste des archives retournée par une recherche multicritères, l'utilisateur a alors la possibilité de sélectionner une référence et de consulter différents éléments de l'archive :

- Le résumé de l'archive présentant :
  - date de dépôt,
  - empreintes,
  - métadonnées…
- le scellement de l'archive
- les métadonnées
- l'objet d'archives

A noter que l'accès à l'objet d'archives nécessite une habilitation particulière.

Avant de présenter l'archive sélectionnée, le système recalcule l'empreinte de l'Objet d'archives et s'assure qu'elle est identique à celle contenue dans l'archive, apportant ainsi implicitement la preuve de l'intégrité de l'Objet d'archives.

Selon la nature de l'Objet d'archives et l'application de consultation, la consultation de l'objet d'archives résulte en une visualisation, un téléchargement ou un transfert par messagerie. Dans tous les cas, la donnée consultée est strictement identique à la donnée initialement confiée.

5.2.3 Communication (ou extraction) en nombre

Sur demande et aux conditions financières prévues au contrat, le client peut demander la communication d'un grand nombre d'archives.

Les archives peuvent être communiquées sous l'un des deux formats suivants :

- format de dépôt (objet d'archives et métadonnées fournies)
- container Archive Docaposte Arkhineo comportant l'objet d'archives, les métadonnées et les éléments de preuves : horodatage, scellement, cycle de vie de l'archive, etc.

Le choix du support de cette communication se fera en accord entre le client et la Société.

5.2.4 Certificat de conformité à l'original

Un document dénommé « attestation d'archivage » peut être généré automatiquement via les interfaces de consultation en fonction des droits associés à l'utilisateur.

Ce document prend la forme d'une attestation au format PDF présentant la partie lisible des éléments de preuve associés à l'archive : Identifiant Unique d'Archive et autres identifiants, Métadonnées, Déposant, cycle de vie, Statut, Empreintes, Horodatage.

Il fait l'objet d'une signature électronique effectuée à l'aide d'un certificat émis par l'autorité de certification Docaposte Arkhineo. Les éléments du certificat de signature utilisé sont également présentés dans le document lui-même.

5.3 Réversibilité

Les Archives pourront, à la demande du client, lui être restituées en totalité, avant l'expiration de la durée de conservation, selon les modalités techniques et financières prévues au contrat.

5.3.1.1 Restitution

Dans ce cadre, la Restitution (Communication de l'ensemble des archives suivie de leur Destruction), aux conditions techniques et financières prévues au contrat, libérera le Tiers-archiveur de son obligation de Conservation des Archives.

Le format et le support de la restitution suivent les règles de la communication en nombre (cf. § 5.2.3).

5.3.1.2 Communication

La Communication de l'ensemble des archives, aux conditions techniques et financières prévues au contrat, ne modifie pas la durée de conservation prévue au contrat. Le Tiers-archiveur continue d'assumer ses obligations de Conservation des Archives.

5.4 Fin de vie

Le contrat liant Docaposte Arkhineo à son client prévoit :

- une durée de service,
- une durée de conservation pour les données confiées.

5.4.1 Durée de service

Le Contrat de Service est conclu pour une durée ferme (par exemple trois ans) à compter de la date de signature du contrat.

Le Contrat est généralement renouvelable par tacite reconduction par période identique, sauf dénonciation par l'une ou l'autre des parties.

Pendant la durée du service, le client peut déposer des archives aux conditions prévues par le contrat (conditions financières, conditions techniques…).

Les archives conservées n'ayant pas atteint la fin de la période de conservation peuvent être consultées librement par les personnes autorisées (cf § 5.2).

5.4.2 Durée de conservation

La durée de conservation des Archives, sauf stipulation contraire, est celle prévue au contrat (par exemple 10 ans), Docaposte Arkhineo s'engageant expressément à respecter ce délai de conservation, quelle que soit l'évolution des relations contractuelles entre les Parties.

5.4.3 Consultation au-delà de la durée de service

Le client pourra bénéficier, à sa demande, au-delà de la durée de service, et jusqu'à la fin de la période de conservation, d'un service de consultation aux conditions indiquées au contrat. Pour ce faire, le client doit maintenir ses moyens d'accès et continuer à souscrire, auprès de Docaposte Arkhineo, aux prestations annexes lui permettant la consultation (Abonnement API, portail, etc.)

À tout moment, le client pourra également demander la Restitution, ou la Communication de la totalité des archives, comme indiqué au § 5.3 - Réversibilité.

5.4.4 Restitution, destruction ou prorogation en fin de période de conservation

Selon la fréquence prévue au contrat (par exemple annuellement), Docaposte Arkhineo demande à son client ses intentions concernant le sort à donner aux archives ayant dépassé la durée de conservation prévue. Celui-ci peut demander, pour les archives concernées :

- La Destruction,
- La Restitution des archives s'accompagnant d'une destruction,
- La prorogation pour une période de conservation supplémentaire (par exemple un an) aux conditions prévues au contrat.

5.4.4.1 Cas particulier des clients du client

Dans le cas où le client a informé Docaposte Arkhineo qu'il archivait des documents numériques pour le compte de ses propres clients, à l'issu des relations contractuelles, soit le client, soit son propre client, pourra demander la Restitution ou la Destruction des Archives.

Le client devra avoir préalablement communiqué au Tiers-archiveur :

- Les Métadonnées permettant de distinguer les archives de ses propres clients,
- L'identité précise de ses propres clients.

Si à l'issue de la relation contractuelle entre le client et son client, ce dernier souhaite continuer à bénéficier du service d'archivage, il devra souscrire un contrat ADE avec Docaposte Arkhineo.

5.4.4.2 Cas particulier des archives publiques

Dans le cas de la conservation d'archives publiques (courantes et intermédiaires), le sort des archives en fin de période de conservation est systématiquement soumis au contrôle scientifique et technique de l'Etat, de même que toute opération anticipée sur l'archive.

En vertu des articles 2, 3 et 4 du Décret n°79-1037 du 3 décembre 1979, (article 2 modifié par Décret n°2006-1828 du 23 décembre), le contrôle scientifique et technique de l'Etat est assuré par des entités différentes en fonction de l'origine des archives :

- Par les services d'archives des affaires étrangères pour les « archives provenant de l'administration centrale, des postes diplomatiques et consulaires et des établissements placés sous l'autorité du ministre des affaires étrangères » ;
- Les services d'archives du ministère de la défense pour les « archives provenant de l'ensemble des forces, services, établissements et organismes des armées ainsi que des services et établissements dont le rattachement aux services d'archives de ce ministère est prévu par décret ».
- Par la direction des Archives de France pour « les archives des services et établissements publics de l'Etat ainsi que des autres personnes morales de droit public, des organismes de droit privé chargés de la gestion des services publics ou d'une mission de service public, des minutes et répertoires des officiers publics ou ministériels ».

A l'élaboration du contrat client, Docaposte Arkhineo identifie le type d'archive conservées et l'autorité compétente quant à la gestion de ces archives. Pour toute opération de restitution, destruction ou prorogation, le visa d'approbation émanant de l'entité compétente est systématiquement exigé du client.

Ainsi, pour les archives gérées par la direction des Archives de France, Docaposte Arkhineo demande à son client de fournir, par lettre recommandée avec accusé de réception, le visa provenant, en fonction des archives concernées, des services de la direction des Archives de France, des inspecteurs généraux des Archives de France, des chefs des missions des archives ou des directeurs des services départementaux d'archives compétents.

5.5 Modification d'archive

La modification d'une Archive est contraire au principe d'intégrité d'un service d'archivage. Le service de Docaposte Arkhineo n'autorise en aucun cas la modification d'une Archive, ce qui le rend conforme à la loi du 13 mars 2000 modifiant le droit de la preuve.

Cependant, selon le contexte applicatif, il peut être utile d'archiver une nouvelle version d'un document référençant la version précédente.

5.6 Destruction d'archive

Le Client pourra, sur demande expresse, réclamer la Destruction d'une ou plusieurs archives parfaitement identifiées.

La Destruction est alors réalisée par la Société après confirmation de la part du Client.

Que l'on soit dans le contexte d'une demande exceptionnelle ou à l'échéance de la durée de Conservation d'une Archive, la destruction de chaque Archive consiste en la réalisation des actions suivantes ; celles-ci étant effectuées pour l'ensemble des exemplaires, sur les deux sites primaires ainsi que sur le site de sauvegarde :

- Désindexer et détruire les métadonnées descriptives
- Désindexer et détruire les métadonnées applicatives
- Détruire l'objet-donnée

Cette destruction s'effectue à l'aide d'un algorithme d'effacement définitif par réécriture, faisant partie des algorithmes recommandés dans le guide d'application Z42-019 de la norme Z42-013.

Seul le journal de cycle de vie de chaque Archive est maintenu, par conservation du scellement de l'Archive. Ce scellement ne contient plus aucun élément fourni par le déposant.

Après Destruction, la Société remet au Client une Attestation de Destruction. Cette attestation n'est constituée et délivrée qu'à l'issu de la destruction de l'ensemble des copies de l'archive, dont la copie sur site de sauvegarde. Cette dernière copie présentant systématiquement, et par sécurité, un retard glissant de 7 jours sur les sites principaux, l'attestation ne peut être délivrée avant ce délai.

5.7 Gel et dégel d'archives

Le Client pourra, sur demande expresse, réclamer le gel ou le dégel d'une ou plusieurs archives parfaitement identifiées.

Le gel ou le dégel est alors réalisé par la Société après confirmation de la part du Client.

Lorsqu'une archive est gelée, elle est automatiquement exclue de toute opération de fin de vie, de prorogation/abrégement ou de destruction. Le déroulement du cycle de vie est suspendu pour cette archive.

Lorsqu'une archive est dégelée, sa date de fin de vie est repoussée de la durée du gel. L'archive est alors de nouveau sujette aux opérations de fin de vie, de prorogation/abrégement ou de destruction.

Une attestation est remise au client à l'issu de l'opération.

5.8 Prorogation/abrégement

Le Client pourra, sur demande expresse, réclamer la modification de la durée de vie d'une ou plusieurs archives parfaitement identifiées.

Cette modification est alors réalisée par la Société après confirmation de la part du Client, et tracée dans le cycle de vie des archives prorogées/abrégées.

Une attestation est remise au client à l'issu de l'opération.

6 PRINCIPES ORGANISATIONNELS

6.1 Les engagements du Tiers-archiveur

Les engagements que prend Docaposte Arkhineo, en tant que Tiers-archiveur, vis-à-vis de son client sont matérialisés par la signature d'un contrat comportant :

- la description du service souscrit par le client,
- une annexe financière détaillant les conditions financières de la fourniture du service. Celles-ci dépendent généralement de la volumétrie et de la durée de conservation,
- un *SLA* fixant les engagements précis de qualité de service et de support accompagnant le service,
- une annexe technique définissant les spécifications techniques externes du service ainsi que les modalités techniques d'accès aux éléments de service.
- Dans le principe, Docaposte Arkhineo en tant que Tiers-archiveur a une double obligation :
- une **obligation de résultat** sur la conservation et la restitution intègre des données confiées,
- une **obligation de moyens** sur les accès aux éléments de service (Dépôt/Capture, Recherche, Consultation etc.).

Ces principes se déclinent en principes organisationnels décrit ci-dessous.

6.2 Parties prenantes

Les parties prenantes du service d'archivage sont :

- La Société **Docaposte Arkhineo**, agissant en qualité de fournisseur du service d'archivage pour ses Clients ;
- Le **Client**, ayant souscrit au service d'archivage Arkhineo ;
- **Docaposte**, agissant en qualité de gestionnaire avec les hébergeurs Data4 et Equinix constituant les deux sites Actif/Actif Docaposte Arkhineo ;
- **Le GIE Informatique CDC**, agissant en qualité d'hébergeur, fournissant l'infrastructure d'hébergement de sauvegarde au sein de la Caisse des Dépôts et Consignations.

6.3 Conservation intègre sur la durée convenue

Docaposte Arkhineo s'engage à présenter, pendant toute la durée de conservation convenue, tout Objet d'archives, référencée par un IUA contenu dans un ARF, après en avoir vérifié l'intégrité.

Pour garantir la conservation sur la durée convenue, lors de la capture des données, 4 exemplaires de l'archive scellée, comportant les données, les métadonnées et les empreintes sont enregistrés d'une manière synchrone et en parallèle sur 4 supports distincts équi-répartis sur deux sites de production indépendants.

Une copie de sécurité est également réalisée d'une manière asynchrone vers le site de sauvegarde.

C'est à la réception de l'Archive, qu'optionnellement un **Acquittement Technique** est retourné au client attestant la bonne réception par Docaposte Arkhineo de l'archive.

L'engagement de conservation et de restitution de Docaposte Arkhineo, concernant une archive particulière, n'est pris qu'à partir du moment où **l'Accusé de Réception Fonctionnel** a été émis explicitement pour l'Archive. Pour le client, l'Accusé de Réception Fonctionnel représente la preuve d'archivage de la donnée.

Docaposte Arkhineo s'engage à disposer de 4 exemplaires de l'archive scellée répartis sur deux sites distincts ou de revenir à cette situation dans les meilleurs délais.

Le site de sauvegarde comporte une copie de sécurité de toutes les archives scellées présente sur les deux sites de production.

Des processus réguliers s'assurent de la disponibilité et de l'intégrité de toutes les archives (cf. § 6.3.2.1).

De plus, à chaque accès à une archive, un nouveau calcul d'empreinte est réalisé et comparé à l'empreinte initiale, garantissant ainsi l'intégrité de l'archive à chaque consultation.

6.3.1 Disponibilité de la plateforme

6.3.1.1 Haute disponibilité

Le Service d'Archivage Electronique Sécurisé de Données Numériques (SAE) est disponible 24 heures sur 24 et 7 jours sur 7. Conformément à la SLA signée avec chaque client, la Société s'engage sur des taux de disponibilité (largement supérieurs à 99 %) à la fois pour le service de capture et pour le service de consultation.

Ces taux de disponibilité sont atteints par la mise en œuvre de technique de haute disponibilité s'appuyant à la fois sur de la redondance à tous les niveaux et sur de la répartition de ces composants sur deux centres de calcul distincts et indépendants.

6.3.1.2 Performance

La conception du système garantit que les performances en dépôt comme en consultation restent constantes, indépendamment du volume d'archives géré par le système ou contenu dans le Coffre-fort concerné.

6.3.1.3 Support client

La Société met à la disposition de ses clients un support permettant de les assister dans l'utilisation du produit et de traiter les incidents. Des procédures d'enregistrement d'incident, d'escalade et d'information du client sont formalisées dans la SLA signée avec chaque client.

L'analyse des éléments enregistrés au moment de la remontée des incidents permet de mesurer le respect des engagements de disponibilité pris par la Société.

6.3.2 Sécurité

La sécurité des données confiées est une préoccupation permanente de Docaposte Arkhineo.

Cette sécurité concerne en premier lieu tous les aspects de la Sécurité des Systèmes d'Informations, en particulier :

- Sécurisation du réseau (Firewall, VPN, etc.)
- Sécurisation des accès (authentification par certificat X509, filtrage IP, politique de mot de passe, etc.)
- Sécurisation des transmissions (HTTPS, TLS, etc.)
- Procédures d'exploitation
- Plan de continuité de l'activité
- Sécurité en matière de développement et maintenance des applications

La sécurité concerne également les aspects spécifiques des Données Numériques dans un Systèmes d'Archivage Electronique :

- Intégrité
- Pérennité
- Confidentialité
- Traçabilité

6.3.2.1 Intégrité

L'empreinte numérique scellée dans l'archive est contrôlée à chaque consultation de l'archive garantissant ainsi que l'Objet d'archives présenté est bien identique à celui déposé.

De plus, des processus réguliers parcourent l'ensemble des archives, sur une base trimestrielle, pour s'assurer du maintien de la qualité des supports, de la disponibilité et de l'intégrité des différents exemplaires de l'archive.

6.3.2.2 Pérennité

En cas de défaillance d'un support entraînant la perte d'au moins un exemplaire de l'archive, la reconstruction du ou des exemplaires manquants est lancée dans les meilleurs délais, au besoin en utilisant la copie de sécurité, pour revenir le plus rapidement possible aux 4 exemplaires disponibles par archive. La procédure de reconstruction s'assure à tout moment du maintien de l'intégrité de l'archive en utilisant des processus adaptés, en recalculant l'empreinte de chaque nouvel exemplaire et en la comparant à l'empreinte initiale (celle contenue dans l'ARF).

6.3.2.3 Confidentialité

En tant que Tiers Archiveur, Docaposte Arkhineo s'engage à ne pas analyser et retraiter les Données Numériques confiées par son client. Ainsi, Docaposte Arkhineo ne procède en aucun cas à une quelconque analyse sémantique du contenu de l'Objet d'archive. Seul le format du fichier est contrôlé et validé : c'est-à-dire la conformité de la structure du fichier au regard des spécifications du format.

Seules les métadonnées, associées à l'Objet d'archives sont analysées et traitées et exploitées pour permettre les contrôles de cohérence et l'indexation.

Le service d'archivage met en œuvre des techniques de cloisonnement et d'habilitation permettant de s'assurer que seules les personnes autorisées peuvent accéder à une archive.

6.3.2.3.1 Confidentialité renforcée

Dans le cas où le client souhaiterait un niveau de confidentialité renforcé, celui-ci est encouragé à chiffrer, avant le dépôt, l'Objet d'archives. Ce procédé, sous le contrôle exclusif du client, lui assure une parfaite confidentialité des informations confiées dans toutes les circonstances.

À noter, que les métadonnées étant utilisées pour la gestion de l'archive, celles-ci devront comporter les informations nécessaires à son indexation et sa recherche.

6.3.2.4 Traçabilité

Dans un système d'archivage, la traçabilité est assurée par la journalisation. Cette fonction consiste à enregistrer, d'une manière automatique tous les événements intervenant dans le système en les chainant les uns aux autres.

La totalité des journaux se décompose en deux ensembles.

6.3.2.4.1 Journal du cycle de vie des archives

Des interfaces utilisateurs permettent la recherche et la consultation dans ce journal aux personnes autorisées.

Ce journal présente les traces de toutes les actions concernant le cycle de vie de chaque archives, notamment :

- Le dépôt d'archives ;
- La prorogation d'archives ;
- La destruction d'archive ;
- La restitution d'archive ;
- Le sur-scellement d'archive ;
- ...

On y trouve par ailleurs des traces de niveau supérieur liées :

- Aux demandes de traitement sur un ensemble d'archives ;
- Aux attestations de fin de traitement sur un ensemble d'archive ;
- Aux contrôles d'intégrité réalisés en tâche de fond.

Enfin, on y trouve les traces de toutes les modifications de configuration des espaces d'archivage :

- profils d'archivage (description des métadonnées, durée de conservation par défaut, etc.) ;
- modifications des comptes utilisateur ;
- modification des habilitations.

6.3.2.4.2 Journal des événements

Une partie du journal des évènements est accessible aux utilisateurs disposant de droits spécifiques. Cette portion du journal comprend principalement :

- Toute recherche réalisée (recherche système, par métadonnée, avancée) ;
- Tout comptage d'archive (nombre, volume) ;
- Toute consultation d'archive (archive complète ; Objet d'archive, métadonnées, etc.)

Les autres constituants du journal des évènements sont globaux à l'ensemble de la plateforme, et ne sont consultables que par les administrateurs Docaposte Arkhineo autorisés.

Ils enregistrent tous les événements systèmes intervenant sur la plateforme. Ils permettent, par analyse ultérieure, en cas d'audit, de reconstituer l'historique des événements systèmes des composants de la plateforme.

Y sont consignés :

- Les évènements relatifs à l'exploitation de l'applicatif : les ajouts de matériels ou d'unités de stockage, les remplacements de matériels ou d'unités de stockage, les allocations d'espace, les arrêts et redémarrage des services ;
- Les évènements relatifs à la sécurité : traces de l'ensemble des accès et tentatives d'accès au SAE ;
- Les évènements relatifs au système : mises à jour des systèmes, erreurs systèmes, traces techniques des logiciels employés, traces d'envoi des journaux d'ARF notamment.

6.3.3 Réversibilité

L'ensemble des processus mis en œuvre dans le SAE respecte le principe fonctionnel de réversibilité (cf. § 5.3).

Ainsi l'Objet Données et les métadonnées associées ne subissent aucune transformation qui ne permettrait pas la restitution les données et les métadonnées dans leur format de dépôt.

Cette réversibilité concerne la restitution de l'ensemble des données confiées.

Les archives peuvent être restituées sous l'un des deux formats suivants :

- format de dépôt (objet d'archives et métadonnées fournies)
- container Archive comportant l'objet d'archives, les métadonnées et les éléments de preuves : horodatage, scellement, cycle de vie de l'archive, etc.

Le choix du support de cette communication se fera en accord entre le client et la Société.

Le processus de restitution correspondant à une demande répondant aux conditions de Réversibilité s'applique selon les conditions prévues au contrat signé par le client.

6.3.4 Validation et conservation des signatures et cachets électroniques qualifiés

Docaposte Arkhineo, en complément de son Service d'Archivage Electronique Sécurisé de Données Numériques, propose un **Service de Validation et Conservation des Signatures et cachets électroniques qualifiés / non qualifiés** des documents déposés.

Lorsque le client a souscrit à cette offre, les signatures sont alors validées lors du dépôt, et les attestations de validation de signatures et cachets sont conservées avec la même Politique d'Archivage que le document signé, renforçant ainsi la valeur probante du document, sans nécessiter de procédure particulière de maintien dans le temps de la validité de la signature.

Les politiques de validation et de conservation des signatures et cachets électroniques qualifiés/non qualifiés sont publiquement disponibles à l'adresse : https://arkhineo.com/fr/ressources/telechargements-pdf/

Les principes organisationnels présentés au sein de la présente politique, associés aux dispositions des politiques de conservation et de validation suscitées, valent déclaration de pratiques de conservation et de validation des signatures et cachets électroniques qualifiés / non qualifiés.

6.4 La responsabilité du client

Le Service proposé par le Tiers-archiveur s'inscrit généralement comme une brique technologique d'une fonction d'Archivage d'une société. Le SAE appartient donc a un processus global visant à organiser et gérer le cycle de vie des documents de l'entreprise.

Il est donc de la responsabilité du client de s'assurer en amont et en aval que le Service réponde bien aux objectifs fixés.

La suite de cette section présente quelques sujets, de la responsabilité du client, qui doivent nécessairement être traités pour que la fonction d'Archivage Electronique, répartie entre le Tiers-archiveur et le client, remplisse correctement ses objectifs.

6.4.1 Politique d'Archivage

Le client doit se doter d'une Politique d'Archivage, en prise avec ses processus métiers, visant à définir :

- une typologie des documents à Archiver
- leur classement (confidentialité, responsabilité, fonction, engagement, valeur, volumétrie, etc.)
- les contraintes sur le cycle de vie du document (Accès, Conservation, Destruction, etc.)
- la politique de sécurité (Authentification des accès, sécurisation des communications, etc.)
- etc.

Cette Politique d'Archivage devra être compatible avec la Politique d'Archivage du Tiers-archiveur.

6.4.2 Format des données

L'intelligibilité du Document Electronique dans le temps repose en grande partie sur la possibilité d'exploiter son format tout au long de sa durée de conservation. Il est donc de la responsabilité du client de sélectionner les formats cibles d'archivage parmi la liste des formats préconisés par Docaposte Arkhineo.

Le Tiers-archiveur pourra étudier et convenir, avec son client, d'un éventuel processus de conversion.

Concernant les formats cibles d'archivage, les recommandations suivantes peuvent être faites.

Afin que le système soit administrable sur le long terme, il convient de ne retenir qu'un nombre restreint de formats cibles pour l'archivage.

Les règles de sélection de ces formats cibles sont les suivantes :

- le format doit reposer sur une norme nationale, européenne ou internationale ;
- dans le cas où le format ne repose pas sur une norme, les spécifications de ce format doivent être publiques et facilement accessibles ;

- le format doit être très largement répandu en termes d'usage ;
- la stabilité du format doit être "maximum", c'est-à-dire que le renouvellement des versions doit être exceptionnel ;
- il doit exister au moins 2 logiciels, d'éditeurs différents, disponibles sur le marché français ou européen qui exploitent ce format ou il doit exister un logiciel en "Open Source" qui gère ce format. Ces logiciels doivent a minima permettre l'affichage, et l'impression des documents ;
- il ne doit pas y avoir de licence pour obtenir les spécifications ou pour écrire des logiciels qui exploitent ce format ;

6.4.3 Versement

Lors du versement d'un Objet d'archives, Il est de la responsabilité du client de s'assurer de la qualité du dépôt. Cela concerne en particulier l'authenticité du document, son origine, son statut (validé, approuvé, signé ...) la conformité du document au format prévu, la validation de la signature.

La constitution des métadonnées accompagnant l'Objet d'archives et leur transmission avec l'Objet d'archives sont également sous la responsabilité du client, lui seul est à même de s'assurer de la conformité de ces métadonnées relativement à l'Objet d'archives et à la politique d'Archivage du client.

À noter qu'un mauvais contrôle des métadonnées en amont du versement, peut résulter en une « perte » de l'archive, celle-ci ne pouvant être retrouvée et donc accédée.

6.4.4 Vérification des Accusés de réception

Il appartient au client de contrôler, sur le Journal des ARF, les Documents Electroniques effectivement reçus et correctement traités par le SAE. Seuls les Objets d'Archive figurant dans le Journal des ARF seront accessibles par les éléments de service du SAE.

Un Objet d'archives qui aurait été versé et qui n'apparaît pas dans le Journal des ARF, devra être redéposé. Il faudra s'assurer que l'éventuelle anomalie à l'origine de la non-prise en compte de l'Objet d'archives a bien été corrigée.

La responsabilité du Tiers-archiveur ne pourra être recherchée pour un Objet d'archives qui n'aurait pas fait l'objet d'un ARF.

6.4.5 Vérification des signatures

Toutes les signatures des documents signés provenant de Docaposte Arkhineo, comme les accusés de réception fonctionnels, devront être vérifiées. Seule cette vérification garantit :

- l'intégrité du document signé,
- l'origine du document,
- sa validité

Le client doit donc s'assurer, dans les meilleurs délais, que le document reçu de Docaposte Arkhineo est bien conforme.

7 PRINCIPES DE MISE EN ŒUVRE

7.1 Échanges entre le Tiers Archiveur et le client

Les échanges entre le client et le Tiers Archiveur s'effectuent par l'intermédiaire de liens de télécommunication sécurisés préalablement définis en accord avec le Tiers Archiveur.

Ces liaisons peuvent utiliser :

- des liaisons spécialisées,
- des liaisons à l'Internet.

Les équipements jusqu'à la plateforme du Tiers Archiveur sont sous la responsabilité du client. Celui-ci doit s'assurer de la disponibilité d'une liaison suffisante (bande passante, disponibilité, fiabilité) pour permettre le versement et la consultation de ses Archives.

La sécurisation des liaisons (chiffrement, contrôle d'intégrité et authentification) est assurée conjointement par le Tiers Archiveur et les équipes techniques du client.

7.2 La sécurité

L'administration et l'organisation de la sécurité s'appuient sur une démarche globale de l'entreprise se situant au cœur du métier de Tiers-archiveur.

Ci-dessous quelques principes qui sous-tendent la gestion de la sécurité du Service d'Archivage Electronique Sécurisé de Données Numériques de Docaposte Arkhineo.

7.2.1 Politique de Sécurité de l'Information (PSI) et Plan de Continuité d'Activité (PCA)

Docaposte Arkhineo possède et maintient une Politique de Sécurité de l'Information. C'est un document classé confidentiel entreprise qui définit le cadre général de la démarche sécurité de la Société et marque l'engagement de la Direction Générale.

La Société a également conduit une analyse des risques permettant d'identifier les actifs essentiels et d'étudier les menaces sur ces actifs pour évaluer les risques.

La PSI ainsi que l'analyse des risques ont permis de produire des documents internes formalisant l'ensemble des éléments stratégiques, les directives, les procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du système d'archivage et la continuité de l'activité.

Un Plan de Continuité d'Activité est également maintenu à jour. Il comporte l'ensemble des mesures visant à assurer, selon divers scénarios de crise, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise puis la reprise planifiée des activités.

7.2.2 Développement logiciel

D'un point de vue stratégique, Docaposte Arkhineo a décidé de maîtriser son outil de production. Cela se traduit par la mise en œuvre d'une application Coffre-fort Electronique® développée par Docaposte Arkhineo.

Docaposte Arkhineo ne dépend donc d'aucun éditeur de logiciel pour son outil de production.

7.2.3 Sécurité physique et environnementale

Le service d'Archivage Sécurisé de Données Numériques (ADE) repose sur une architecture technique constituée des trois sites décrits ci-après.

Ces trois sites sont localisés dans des bâtiments sécurisés propriété de la Caisse de Dépôts et Consignations. L'exploitation des infrastructures est assurée par l'hébergeur.

Ces sites comportent des équipements de :

- sécurité anti-intrusion,
- détection et extinction incendie,
- alimentation électrique redondante avec groupes de secours,
- climatisation redondante,
- système de recyclage d'air.

7.2.3.1 Deux sites actifs

Docaposte Arkhineo dispose de 2 sites en fonctionnement dit actif/actif localisés chez les hébergeurs Data4 Marcoussis (91) – France et Equinix St-Denis Porte de Paris - France. Chacun de ces deux sites est indépendant et autonome, avec ses propres sources d'énergie et de climatisation redondées.

Chacun ayant également des accès télécommunications dédiés avec un système de bascule automatique, chez les fournisseurs d'accès, en cas de rupture d'un lien.

7.2.3.2 Site de sauvegarde

Ce troisième site, localisé chez les hébergeurs CDC-EDF à Val-de-Reuil (27) - France, est distant de plus de 100 Km des sites actif/actif. Il reçoit les copies de sécurité des archives et les sauvegardes des configurations.

7.2.4 Contrôle d'accès

Des mesures de contrôles d'accès strictes sont prises pour n'autoriser l'accès aux salles machines qu'aux personnels autorisés de Docaposte Arkhineo et parfaitement identifiés.

L'accès à l'administration des différents systèmes et des applications composants le système d'archivage est strictement contrôlé et réservé aux seuls personnels autorisés de Docaposte Arkhineo à l'exclusion de toute personne extérieure (y compris fournisseurs, mainteneurs, hébergeurs, etc.).

7.2.5 Sécurité des matériels

Lors du choix des équipements, de leur installation et de leur exploitation un focus particulier est réalisé sur les aspects sécurité.

7.2.6 Sécurité des logiciels

Avant d'être mis en exploitation, les logiciels ou leurs nouvelles versions font systématiquement l'objet d'une procédure de qualification permettant de s'assurer de leur conformité relativement :

- à leur spécification,
- à leur futur environnement de production,
- à leurs performances attendues.

7.2.7 Sécurité des systèmes d'information

Conformément à la Politique de Sécurité de l'Information et des documents opérationnels associés, la Société met en œuvre un ensemble de moyens de protection renforcés (redondance des équipements, firewall, VPN, contrôle d'accès etc.), destinés à assurer la sécurité du Système d'Archivage.

7.2.8 Sécurité liée aux ressources humaines

Lors du recrutement et de l'intégration, Docaposte Arkhineo sensibilise et forme ses personnels aux aspects sécurité du métier de Tiers-archiveur ainsi qu'à la politique de sécurité de la Société (PSI).

De plus, une clause concernant le secret professionnel est systématiquement intégrée au contrat de travail de tout salarié de l'entreprise.

8 PRINCIPES TECHNIQUES

8.1 Horodatage

Une contremarque de temps lie la représentation d'une donnée à une mesure du temps émanant d'une source de temps fiable.

La preuve de dépôt (l'ARF), comportant le scellement avec la date de dépôt, signée du Tiers-archiveur constitue une contremarque de temps établissant ainsi la preuve que la donnée existait à l'instant du dépôt.

8.2 Scellement

Le scellement est réalisé par la signature de l'empreinte de l'archive par une clé privée associée à un certificat fourni par la PKI interne. Ce scellement garantit l'intégrité de l'Objet d'archives.

8.3 Disques réinscriptibles avec moyens cryptographiques

Le support utilisé pour l'archivage des données est le disque magnétique réinscriptible. Associé aux moyens cryptographiques de scellement, ce support est conforme aux recommandations des normes professionnelles de l'archivage numérique.