# CHAP 4- L’OBLIGATION DE SECURISER LES DONNEES NUMERIQUES

1. **LES OBLIGATIONS LEGALES QUI S’IMPOSENT A UN SERVICE INFORMATIQUE EN**

**MATIERE D’ARCHIVAGE :**

* 1. **Définition**

L’archivage électronique peut se définir comme « l’ensemble des actions, outils et méthodes mises en

oeuvre pour conserver à moyen ou long terme des informations dans le but de les exploiter.»

* 1. **L’archivage légal**

L’archivage c'est-à-dire la conservation de documents, est une **obligation légale** pour l’entreprise (documents fiscaux et administratifs)

afin de se prévaloir d'une équivalence entre le support papier et la

forme électronique de l'écrit.

Comment faire valoir juridiquement l’écrit électronique comme preuve au même titre que le papier ? sous 2 conditions :

* garantir l’intégrité du document
* garantir l’identification de son auteur : l’utilisation d’une signature électronique (signature électronique délivrée par un prestataire de certification électronique) authentifie l’auteur du document..

L'archivage électronique, lorsqu'il respecte les dispositions de la norme ISO 14641-1 *(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 au sein d'un système d'archivage électronique (SAE)(Wikipedia*))., apporte des garanties qui peuvent être utilisées dans le cadre d'un

contentieux pour démontrer la valeur probante d'un document => **l’archivage assure l’intégrité, la**

# pérennité, la datation précise et certaine, la sécurisation, l’accessibilité, …

* 1. **La procédure d’archivage**

Pour garantir authenticité et intégrité d’un document, obligation de suivre une procédure : sur des CD- Rom ou DVD non réinscriptibles ou sur des disques durs externes voire DVD Blu-ray ; supports vierges ; provenant de lots différents ; faire la gravure en au moins 2 exemplaires à l’aide d’un logiciel spécifique ; vérifier la lecture de chaque support ; stocker chaque support en des lieux distincts ; tester chaque année les supports pour s’assurer de leur conservation.

L’archivage doit permettre une lecture de ces données indépendante du matériel et des logiciels originels (pb délicat face à l’obsolescence rapide des matériels et logiciels, une préconisation de l’Académie des sciences et de l’Académie des technologies : utiliser différents supports et le refaire tous les 4 ans sur des supports neufs ! coût ???).

En pratique, si l’authenticité ou l’intégrité d’un document est contestée, un expert décidera du caractère probant dudit document et le juge forgera sa décision en fonction du niveau de protection que l’entreprise aura mis en place dans le but de garantir la force probante des données

# L’ARCHIVAGE DES DONNEES A CARACTERE PERSONNEL :

* 1. **Définition de DCP**

Une DCP est une donnée qui permet l’identification directe ou indirecte d’une personne : pas seulement son nom mais aussi sa voix, son image, ses empreintes génétiques ou un n° d’identification, n° de compte bancaire, adresse IP ou encore des renseignements relatifs à la personnalité.

* 1. **Le RGPD et les DCP**

Il définit un nouveau cadre juridique de la protection des DCP ; **il renforce plusieurs grands principes** :

* le principe de licéité, de loyauté et de transparence. La licéité répond à un certain nombre de conditions alternatives au rang desquelles figure le consentement explicite de la personne.
* le principe de limitation des finalités : les données doivent être « collectées pour des finalités déterminées, explicites et légitimes ».
* le principe de « minimisation des données » : les données doivent être « adéquates », « pertinentes », « limitées à ce qui est nécessaire au regard des finalités ».
* le principe d’exactitude : les données doivent être exactes et à jour.
* le principe de limitation de la conservation : La conservation des données doit être limitée dans le temps.

– le principe de sécurité : les données doivent être traitées de manière à en garantir l’intégrité et la

confidentialité.

A ces principes s’ajoute celui de la « **responsabilité du responsable du traitement »** : les organismes doivent désormais s’assurer eux-mêmes de la conformité de leurs traitements au nouveau cadre juridique et pouvoir la démontrer. Ils doivent aussi désigner un délégué à la protection des données ou data protection officer (DPO), chargé de conseiller l’organisme, mais aussi de contrôler la conformité de ses traitements au RGPD. Le RGPD impose également de tenir un « registre des opérations de traitement », dont la CNIL propose un [modèle](https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf).

Contrepartie de la responsabilité, les textes alourdissent les sanctions en cas de non-respect, jusqu’à 20

millions € ou, s’agissant d’une entreprise, 4% de son chiffre d’affaires mondial.

Le RGPD continue à distinguer au sein des DCP les données sensibles : données relatives à l’origine

raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l’appartenance syndicale, à la vie sexuelle ou à l’orientation sexuelle et à la santé, ainsi que des données

génétiques et biométriques

Les données sensibles sont soumises à des conditions de traitement particulières : déclarations et autorisations sont nécessaires auprès de la CNIL

# LES DROITS DES PERSONNES SUR LEURS DONNEES :

Le texte associe des droits pour les personnes concernées par un traitement de données :

\*le droit à l’information préalable : pas de fichier créé à l’insu des personnes concernées.

\*le droit au consentement préalable aux différents traitements

\*le droit d’opposition

\*le droit à l’effacement

\*le droit d’interroger (le responsable du traitement) et d’accéder (aux données qui concernent la personne)

\*le droit de rectification

\*le droit à l’oubli

\*le droit à la portabilité des données qui permet de récupérer les informations fournies sous une forme réutilisable, afin, par exemple, de les transférer à un tiers.

Remarque : pour faire respecter ces droits, la personne peut porter plainte auprès de la CNIL par simple courrier. Règlement amiable recherché puis si nécessaire sanctions de la CNIL.

# NOTIONS DE SECURITE ET DE CONFIDENTIALITE DES DONNEES DE

**L’ENTREPRISE :**

Alors comment protéger efficacement les données d’une entreprise afin de réduire les risques de piratage, les erreurs et malveillances ?

# La sécurité logicielle du système informatique :

* + Le mot de passe.
  + Le pare-feu ou firewall
  + L’anti spam
  + L’antivirus
  + L’audit : il est fortement conseillé de régulièrement réaliser des audits du système de sécurité de l’entreprise dans le but de tester les logiciels de protection, d’identifier les failles de sécurité, de rechercher les tentatives d’intrusion ou attaques internes et externes, de contrôler l’accès aux données…

# La sécurité physique du SI :

* + La gestion des droits d’accès au poste et aux données informatiques
  + La sécurité des locaux
  + La charte informatique de l’entreprise qui précise les obligations des salariés en matière d’utilisation du SI.

# La procédure de chiffrement des données :

* + C’est un procédé permettant de rendre la compréhension possible d’un document à son seul destinataire qui dispose de la clé de chiffrement. Il a été défini dans la LCEN de 2004. Ces moyens de cryptologie ont pour objet de garantir la sécurité du stockage ou de la transmission de données en toute confidentialité, authentification et intégrité.