Pourquoi l'archivage électronique est essentiel à votre activité

1 – Quelle est la différence entre une GED et un SAE ?

Contrairement à l'outil de GED (gestion électronique de documents) qui permet essentiellement le classement et le partage de l'information, le système d'archivage électronique (SAE) préserve la valeur juridique des documents engageants en garantissant leur intégrité et leur recevabilité.
Il constitue un point clé de la pérennité et la conformité à long terme des documents et données électroniques de l'entreprise. En outre, il est le garant de la capacité de l'entreprise à pouvoir faire face aux enjeux d'un contrôle fiscal et plus particulièrement en cas de CFCI (« Contrôle Fiscal des Comptabilités Informatisées »).

2 – En quoi une GED et un SAE sont-ils complémentaires ?

Le SAE ne permet ni de créer ni de modifier un document mais garantie la disponibilité de documents et de donnés intègres dans le temps. Il met en place un classement, des règles de conservation des documents, et permet de détruire un document à la fin de la durée définie de conservation. Les règles mises en place sont calquées à minima sur les durées légales de conservation des documents. Un système de notification alerte le propriétaire du document de l'atteinte de cette échéance de durée de vie afin d'éviter le risque d'une non-conformité au RGPD.

Les deux solutions sont complémentaires dans la mesure où la sélection des documents à conserver dans le SAE peut être facilitée par une GED bien pensée et bien gérée : la GED facilite les activités, le SAE sécurise les actifs de l'entreprise.

3 – Pourquoi le SAE doit-il faire partie des plans de transformation digitale des organisations ?

La mise en place d'une politique de conservation sécurisée des données et documents électroniques est l'une des premières étapes de la transformation numérique des entreprises. Elle permet des processus dématérialisés de bout en bout, notamment pour les parcours de souscription client (contractualisation, achat de biens et services, etc.).

De son côté, l'administration a depuis 15 ans initié une transformation digitale efficace en posant les bases d'un contrôle fiscal renouvelé qui ont induit des changements profonds (FEC, CFCI, PAF, etc). Et demain, la réforme de facturation électronique obligatoire dès 2023 et le « e-reporting » TVA accentue également la nécessité pour les entreprises de conserver et d'archiver de manière sécurisée des données et documents au format électronique.

Pour cela, le SAE offre de nombreux avantages grâce à des datacenters hautement sécurisés : sécurité, accessibilité, confidentialité, conservation à long terme, protection des données, conservation de l'intégrité, validation et préservation des données de signatures électroniques etc. Aucun traitement n'est effectué sur ceux-ci, excepté leur format qui peut être modifié si besoin (en fonction des normes et des mises à jour) sous le contrôle de leur propriétaire et validé, mais le contenu n'est ni regardé, ni analysé, ni altéré.

4 – En quoi le SAE se distingue de la GED en termes de conformité ?

La distinction entre GED et SAE prend tout son sens quand les documents à archiver ont une valeur légale ou réglementaire. En garantissant la sécurité des données archivées et la traçabilité des opérations, le SAE facilite la mise en conformité avec le RGPD.
En matière d'archivage électronique, la référence est la norme NF Z42-013 ou ISO 14641-1.
Elle fixe le cadre de conservation des documents électroniques de manière pérenne, intègre et sécurisée. La traçabilité et l'horodatage de tous les événements du SAE (accès aux documents, demandes de communication, demandes de destruction, documents arrivés à échéance, etc.) permet de répondre pleinement aux exigences de conformité.

5 – Comment assurer la pérennité et la lisibilité des contenus archivés dans un SAE ?

Avec un SAE, l'entreprise règle les questions relatives à la pérennité et aux migrations technologiques, mais aussi à celles concernant la réversibilité et la lisibilité des documents dans le temps. En effet, la pérennité et la lisibilité des documents archivés impliquent l'utilisation de formats de fichiers qui resteront lisibles sur le long terme, mais aussi le contrôle du format au moment du versement. Même si le document est versé dans un format théoriquement pérenne, le SAE permet de s'assurer, grâce à des outils spécifiques, que c'est effectivement le cas, et enclenche un processus de « validation » de ce format. Une procédure obligatoire afin de garantir le maintien de la valeur probante au fil des années.

6 – Pourquoi le SAE facilite le décommissionnement d'applications ?

Décommissionner une application métier consiste à gérer et prévoir sa fin de vie, et à traiter les informations qu'elle contient en vue de leur conservation ou de leur réexploitation éventuelle. Si ces données sont, dès le départ, correctement archivées dans un SAE, elles restent non seulement accessibles, mais il sera également beaucoup plus facile et rapide de retrouver l'information voulue, au moment voulu notamment en cas de CFCI.
L'archivage électronique facilite ainsi le décommissionnement de certaines applications métier (ERP, compta, etc.) qui coûtent chaque année des sommes folles aux organisations et qui pourtant ne sont plus utilisées.

7 – Pourquoi le SAE fait partie des piliers de la cybersécurité ?

L'archivage électronique constitue une solution avantageuse pour prévenir les cyber-attaques. En confiant l'archivage de ces documents à un prestataire certifié, les organisations garantissent la préservation de leur valeur probante. Elles ne pourront pas être suspectées de les avoir manipulés et éviteront, par ailleurs, les désagréments liés aux défaillances des systèmes IT et à l'obsolescence technologique, tout en suivant le rythme des évolutions juridiques et normatives.

Il existe des prestataires de confiance spécialisés dans ce domaine qui possèdent des équipes formées et les certifications ad hoc. Un certain nombre d'autorisations, de normes, de certifications et de qualifications sont indispensables. La certification ISO 27001 (pour les systèmes de management de la sécurité informatique), la NF 461, pour la conformité aux normes Afnor NF Z42-013 et ISO 14641-1 (relatives aux systèmes d'archivage électronique à valeur probante), ou encore le label France Cybersécurité, les qualifications eIDAS ou enfin la certification HDS (pour les données de santé à caractère personnel).