DocuWare

Archivage électronique des documents : normes de sécurité 2020

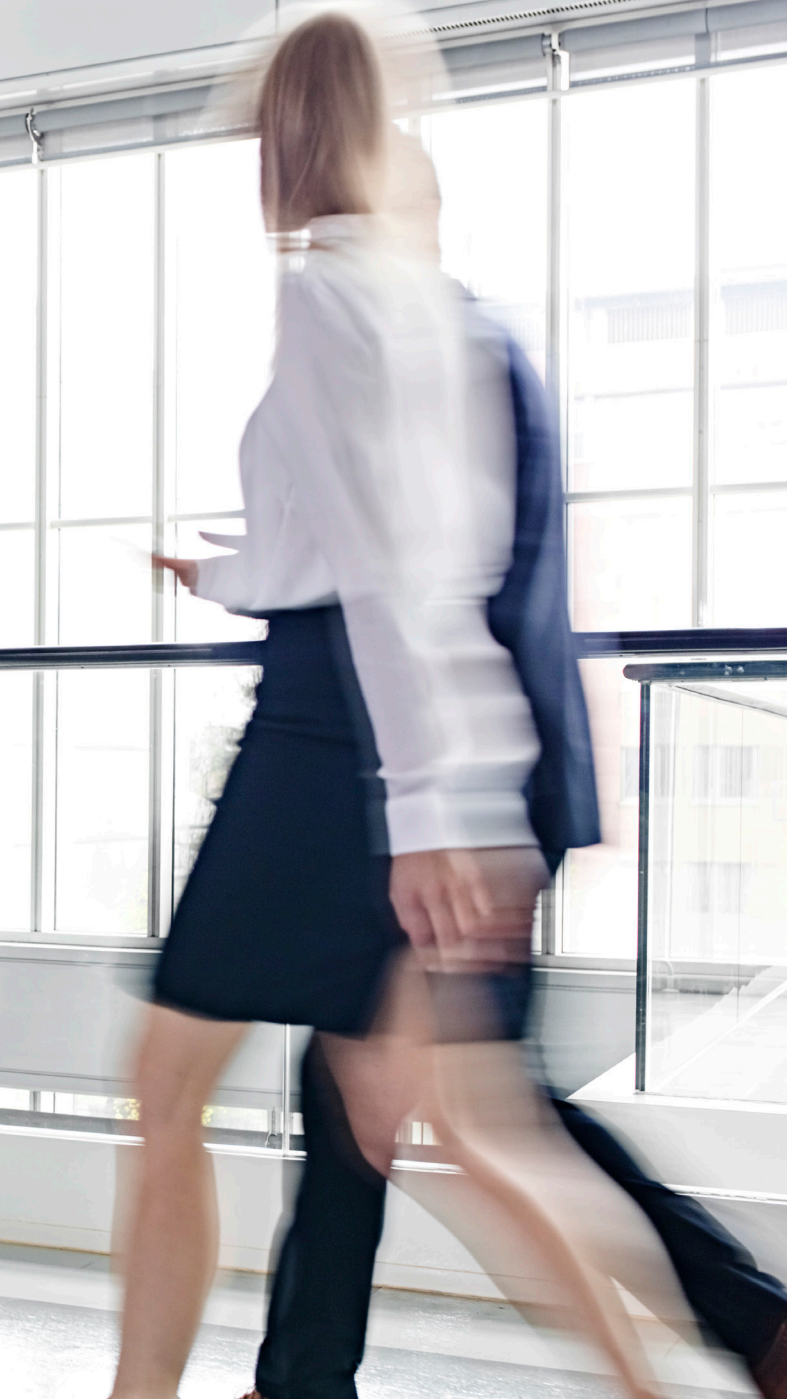
docuware.com

DocuWare

Les failles de sécurité, pertes de données, problèmes liés à la gestion des versions et contentieux relatifs au non-respect des réglementations sont devenus si banals qu'ils semblent faire partie des activités « normales » de l'entreprise.

Toutefois, ces contretemps peuvent aisément être évités. Par souci de simplicité, les organisations optent souvent pour des systèmes de sécurité moins performants, ignorent les réglementations en vigueur ou ne mettent pas en place les processus assurant l'intégrité et la transparence des informations. Les entreprises qui adoptent des mesures de sécurité fiables sont moins susceptibles de s'exposer à de tels risques.

Introduction



Pourquoi la sécurité des documents est-elle essentielle ?

Vos documents sont essentiels au bon déroulement de vos activités. Il est donc crucial que les données qu'ils contiennent soient protégées. Posez-vous les questions suivantes :

Pour les entreprises :

- Sommes-nous protégés contre les fuites accidentelles ou volontaires de données ?
- Sommes-nous protégés contre les attaques externes ?
- Une solution de reprise sur incident est-elle en place ?
- Sommes-nous en mesure de nous défendre contre les accusations de mauvaise gestion des données ?
- Sommes-nous à l'abri de toute amende conséquente ?

Pour les utilisateurs :

- Ai-je librement accès au document requis ?
- Suis-je sûr d'avoir accès à la version adéquate ?
- Puis-je stocker mes informations en toute sécurité, sans que toute personne non autorisée y ait accès. ?
- Est-ce que je dispose d'un processus visant à maintenir des périodes de rétention pour les informations juridiques confidentielles ?
- Suis-je formé pour reconnaître les tentatives d'intrusion ou de hacking ?

Découvrez les normes de sécurité en vigueur pour l'archivage électronique et l'utilisation des documents, et profitez d'un guide pratique pour bien choisir votre éditeur de logiciels GED.

DocuWare

1

Chiffrement et droits d'accès

Comment les données dématérialisées sont-elles sécurisées ? Quels sont les points faibles entre les systèmes ? Comment l'accès aux informations peut-il être contrôlé ? De quelle manière les entreprises se protègent-elles des fuites de données ?

Chiffrement et droits d'accès

DocuWare

Authentification

L'accès aux documents doit se faire uniquement via la saisie d'un nom d'utilisateur (login) et d'un mot de passe uniques. Ainsi, seuls les utilisateurs autorisés peuvent les consulter, et un suivi complet est réalisable (document lu, par qui et quelles actions ont été effectuées).

Trafic

L'ensemble du trafic entre systèmes et composants doit être chiffré au format HTTPS. Tout trafic non sécurisé induit de plus grands risques de piratage. Le chiffrement HTTP n'inclut pas de couche de sécurité SSL et permet donc aux hackers d'intercepter des données critiques (mots de passe, informations financières, etc.).

Contrôle des accès

Un contrôle à niveau multiple est requis pour la gestion des droits d'accès aux documents. Des groupes d'utilisateurs peuvent être associés à des documents partagés. Ces groupes ont besoin de droits spécifiques en fonction des actions qu'ils ont à effectuer. Ces droits doivent également être attribués individuellement.

Par exemple, un membre des RH doit avoir accès à la plupart des documents des employés (CV, évaluations de performances, etc.). Les employés comme leurs managers doivent pouvoir accéder aux évaluations. Les employés doivent également avoir accès à leurs informations financières et d'assurance.

De plus, vous devez être en mesure de limiter l'accès à un document en fonction de ses données d'index (les métadonnées utilisées pour décrire son contenu et son objectif).

Chiffrement

Les documents doivent être chiffrés à l'aide d'une clé de 256 bits minimum. Il s'agit d'un chiffrement de qualité militaire et de la norme actuellement adoptée par le gouvernement américain pour ses données classées secret, qui doivent être protégées contre toute attaque.

DocuWare

2

Redondance et anti-virus

La redondance du stockage constitue un autre élément incontournable de la protection des données. Si un système rencontre des problèmes, celui de secours assure-t-il la continuité des opérations ? Que se passe-t-il si tous les systèmes sont en panne ? Le redondance et la protection des données contre les logiciels malveillants sont indispensables pour assurer la tranquillité d'esprit dans l'entreprise.

Redondance et anti-virus

DocuWare

Redondance active

Les logiciels GED dans le cloud ou on-premise doivent inclure au moins deux niveaux de redondance de stockage. De plus, un troisième niveau de redondance géographiquement distinct assure la continuité des opérations en cas de sinistre.

Il s'agit d'un avantage majeur des systèmes cloud modernes. En tirant parti des services d'infrastructure dans le cloud de fournisseurs tels que Microsoft, les principaux centres de données dans le monde peuvent être utilisés afin de protéger les informations de manière synchrone. Les autres fournisseurs sont Google, Amazon et Oracle.

Souveraineté des données

De nombreuses entreprises tiennent à conserver leurs données dans leur pays d'origine. Ainsi, les organisations américaines préfèrent éviter de stocker leurs données en Amérique du Sud, et les entreprises européennes ne veulent pas que leurs données soient conservées aux États-Unis, à moins qu'elles y fassent aussi des affaires. Les fournisseurs de services dans le cloud doivent s'assurer que les données et leurs sauvegardes restent dans le pays dont les réglementations protégeront le client.

Protection contre les virus et logiciels malveillants

Les cryptovirus sont intégrés aux documents et s'activent à leur ouverture sur un appareil local. Les systèmes de gestion des documents doivent offrir une sécurité fiable contre les attaques malveillantes, de sorte à protéger l'environnement de l'utilisateur et la plateforme logicielle.

DocuWare

3

Politiques de conservation et de mise en conformité

Une fois le chiffrement, les droits d'accès et la redondance du stockage en place, l'entreprise doit décider comment gérer les informations. Les politiques de conservation des données définissent les éléments sauvegardés et leurs modalités de suppression. En vous conformant aux réglementations en vigueur, vous bénéficiez d'un cadre légal pour la bonne gestion des informations.

Politiques de conservation et de mise en conformité

Politiques de conservation des données

Les entreprises sont juridiquement tenues de conserver certains types de documents pendant un nombre d'années spécifique. Par exemple, les factures clients et fournisseurs doivent l'être pendant 10 ans en France, avant de pouvoir être détruites.

À l'époque du papier, ces documents étaient stockés dans des meubles remplis de classeurs, puis détruits page par page à l'aide d'une broyeuse. Si la dématérialisation des documents a changé les processus, les réglementations doivent toujours être respectées. Les systèmes GED doivent inclure les outils nécessaires à leur protection ou à leur destruction prédéfinie, afin d'éviter toute action juridique à l'encontre de votre organisation.

Initiatives principales pour la mise en conformité

La protection du droit des individus a connu un regain d'intérêt suite à la publication de nouvelles lois et réglementations sur la protection des données personnelles.

Quelques exemples :

- **HIPAA :** la loi Health Insurance Portability and Accountability Act protège les consommateurs américains quant à l'utilisation, la divulgation et le stockage de leurs données médicales.
- **CCPA :** la loi California Consumer Privacy Act garantit certains droits de confidentialité, d'accès aux données et de transparence aux citoyens de Californie, aux États-Unis.
- **RGPD :** le Règlement Général sur la Protection des Données est un ensemble de règles et normes européennes visant à protéger les données et les informations à caractère personnel des individus via la gouvernance des données.
- **Sarbanes-Oxley :** loi luttant contre les erreurs de comptabilité et pratiques de rapport frauduleuses grâce à une divulgation précise des informations.

DocuWare

4

Intégrité et audits

L'intégrité des documents doit être maintenue à chaque fois qu'un utilisateur y accède. Appliquer un chiffrement de haut niveau et contrôler très étroitement les droits d'accès ne sert à rien si le document lui-même est corrompu.

Intégrité et audits

Signatures électroniques

Les utilisateurs doivent pouvoir signer leurs documents à l'aide d'une signature électronique légalement valide. Une signature électronique qualifiée représente le niveau de signature le plus sécurisé. Selon le règlement eIDAS de l'UE, la validité légale d'une signature électronique qualifiée est égale à celle d'une signature à la main. Cela permet de s'assurer qu'un fournisseur de services de confiance a délivré un certificat numérique et a authentifié le signataire, et donc que les documents n'ont pas été manipulés. L'automatisation des workflows permet aux utilisateurs d'ajouter automatiquement une signature électronique au cours de leurs processus.

Journalisation des changements

La seule façon de réaliser des audits exhaustifs est de consigner chaque consultation, annotation et statut des workflows pour les documents. Cela permet de bénéficier d'un historique complet, disponible en tant que fichier CSV ou autre format répandu.

Gestion des versions

Maintenir l'intégrité des documents suppose d'être en mesure d'identifier les changements entre chaque version, et de s'assurer que les utilisateurs travaillent toujours sur la version la plus récente. Vous pouvez verrouiller les documents qui ne devraient plus être modifiés, afin de disposer d'un historique précis des dernières modifications.

DocuWare

5

Les normes de sécurité les plus importantes

Plusieurs normes internationales et locales sont à observer en termes de qualité du système, de sécurité et de fonctionnalités. Assurez-vous que le fournisseur de votre choix respecte toutes les réglementations en vigueur.

Les normes de sécurité les plus importantes

Qualité du logiciel et fournisseur de services dans le cloud

- **ISO 9001 :** excellent contrôle de la qualité au niveau de la production/fabrication du logiciel.
- **ISO 15489 :** concepts et principes de gestion des données d'entreprise fiables et éprouvés.
- **ISO 27001 :** exigences les plus élevées en termes de production, de mise en place, de fonctionnement, de surveillance, de maintenance et d'amélioration d'un système de gestion des documents.
- **ISO 27017 :** sécurité optimale dans le cloud ; données protégées contre les accès par des tiers, et accès aux documents réservé au client.
- **CSA :** exigences en termes d'hébergement pour la sécurité, la confidentialité, la mise en conformité et la gestion des risques dans le cadre de la Cloud Controls Matrix de la Cloud Security Alliance.
- **Keypoint Intelligence/Buyer's Laboratory :** analyse indépendante pour les produits de bureau spécialisés.
- **SOC :** SOC (Service Organization Controls) est le nom d'un ensemble de normes applicables aux contrôles d'un fournisseur pour la sécurité, la disponibilité, l'intégrité de traitement et la confidentialité. Les fournisseurs de logiciels dans le cloud (SaaS) sont concernés.
- **NIST SP 800–171 :** normes et consignes liées à la protection des systèmes d'informations des agences fédérales américaines.

Gestion des documents financiers

- **GoBD (Allemagne) :** archivage de long terme inaltérable selon le code fiscal et du commerce allemand (HGB/AO).
- **Agencia Tributaria (Espagne) :** exigences du code fiscal espagnol pour l'archivage de documents scannés.
- **GeBüV/AccO (Suisse) :** ordonnance sur la maintenance et la rétention des comptes.

DocuWare

6

Éléments à prendre en compte pour choisir un fournisseur de services d'archivage électronique

Lorsque vous évaluez les logiciels de gestion électronique de documents (GED), il convient avant tout de vérifier la sécurité proposée par le système en question. Sans cela, ce dernier ne vous servirait à rien, quelles que soient les autres fonctionnalités disponibles.

Éléments à prendre en compte pour choisir un fournisseur de services d'archivage

Dressez une check-list de vérifications à effectuer pour vous assurer que chaque évaluation de la sécurité, de la mise en conformité et des fonctionnalités est exhaustive et équitable.

Le système...

- ✓ ...se sert-il d'identifiants individuels pour l'authentification ?
- ✓ ...envoie-t-il toutes les données entre composants Web via le protocole HTTPS ?
- ✓ ...permet-il d'utiliser des droits d'accès spécifiques aux documents, individus, rôles et groupes ?
- ✓ ...propose-t-il un chiffrement 256 bits moderne ?
- ✓ ...sauvegarde-t-il activement toutes les données, y compris dans un emplacement géographiquement distinct ?
- ✓ ...stocke-t-il les données au sein d'une région assurant leur souveraineté ?
- ✓ ...offre-t-il une protection contre les cryptovirus et logiciels malveillants ?
- ✓ ...permet-il d'appliquer des politiques de rétention ?
- ✓ ...aide-t-il à se conformer aux normes relatives à la gestion des données ?
- ✓ ...conserve-t-il l'intégrité des signatures électroniques ?
- ✓ ...consigne-t-il tous les changements afin de créer un historique complet ?
- ✓ ...permet-il de gérer les versions actives et antérieures des documents ?
- ✓ ...propose-t-il des normes tierce de qualité et de sécurité avérées ?
- ✓ ...permet-il l'intégration avec d'autres systèmes d'entreprise (CRM, ERP, etc.) ?
- ✓ ...assure-t-il la non-répudiation ?
- ✓ ...garantit-il une disponibilité et un temps d'activité optimaux ?
- ✓ ...fournit-il une assistance 24 h/24 et 7 j/7 ?

docuware.com

À propos de DocuWare

DocuWare propose des solutions d'automatisation des workflows et de gestion électronique des documents permettant aux entreprises de tirer le meilleur parti de leurs ressources.

DocuWare

DocuWare Europe GmbH

Therese-Giehse-Platz 2 | 82110 Germering | Allemagne
Téléphone : +49 89 894433-0 | **Fax :** +49 89 8419966
E-mail: infoline@docuware.com

DocuWare Corporation

4 Crotty Lane, Suite 200 | New Windsor, NY 12553 | États-Unis
Téléphone : +1 (845) 563-9045 | **Numéro gratuit :** +1 (888) 565-5907
E-mail: dwsales@docuware.com

DocuWare SARL

17, rue du Colisée | 75008 Paris | France
Téléphone : +33 (0)1 57 19 03 23
E-mail : infoline@docuware.com