cegid

RESSOURCES HUMAINES

Paie : la digitalisation au service de la sécurité des données

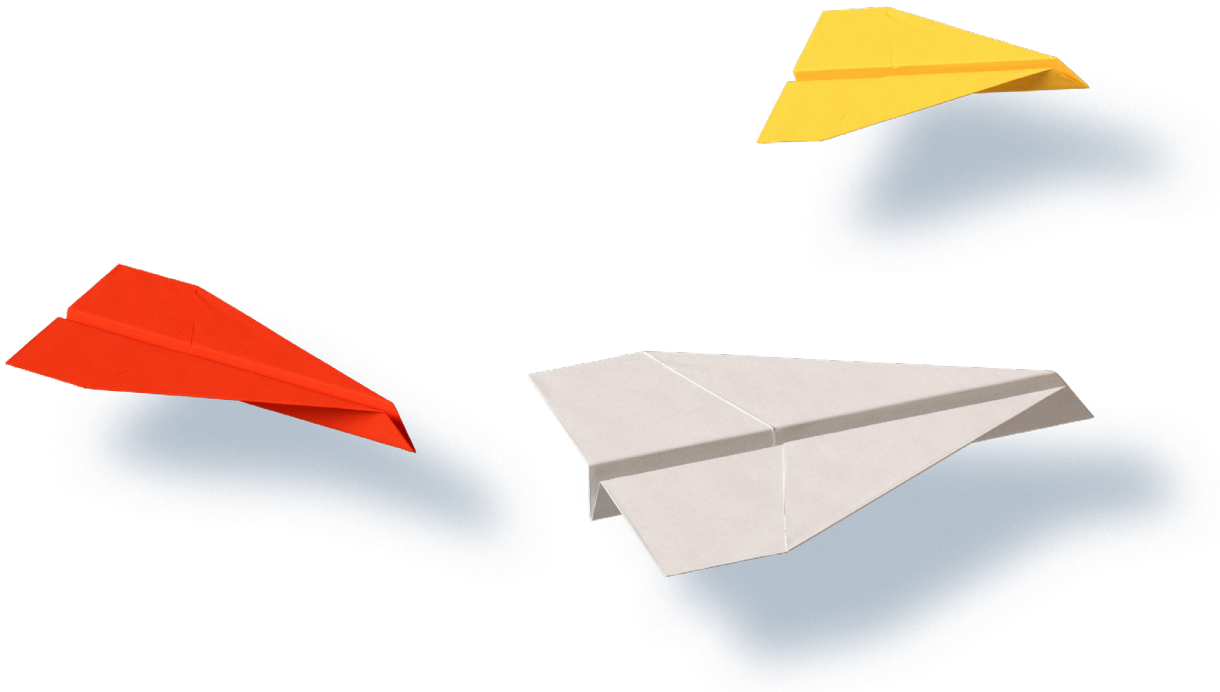
www.cegid.com

sommaire

Édito : digitaliser, oui mais en toute sécurité !

On le sait, la digitalisation transforme en profondeur la vie des services RH. Mais quel impact a-t-elle réellement sur la sécurité des données ? Si cette question se pose dans tous les services de l'entreprise, elle est particulièrement cruciale lorsqu'elle concerne la direction des ressources humaines et les gestionnaires de paie. Les données gérées par les responsables RH sont extrêmement diverses mais également sensibles voire confidentielles : état civil, coordonnées, parcours professionnel, informations bancaires, rémunération, situation familiale et même désormais fiscale sont ainsi présentes dans les bases de données RH.

Lors du déploiement d'un projet paie, la gestion des données, leur sécurité et leur confidentialité doivent figurer parmi les principales préoccupations des DRH. L'enjeu est de mettre la digitalisation au service de la sécurité et de profiter du déploiement d'un nouvel outil pour l'améliorer. Dans ce cadre, une collaboration étroite entre DRH et DSI est nécessaire pour que la digitalisation du service RH se déroule dans les meilleures conditions.



Comprendre la sécurité digitale

La digitalisation, un risque ?

Selon une étude réalisée en 2018 par le cabinet Markess, 71% des décideurs estiment que la digitalisation de leurs processus entraîne des risques relatifs à la sécurité des données. Une méfiance qui repose sur une idée répandue : les données numériques seraient plus vulnérables que les données stockées sur papier. Les décideurs qui partagent cet avis engagent donc la digitalisation de leurs outils à contre-cœur, parce qu'ils la perçoivent comme inévitable. C'est en particulier le cas chez les dirigeants de PME et d'ETI : en 2018, 87% ne considéraient pas la digitalisation de leurs processus comme une priorité stratégique*.

Pourtant, une digitalisation RH réalisée en tenant compte de l'ensemble des risques qui pèsent sur les données personnelles peut au contraire améliorer leur niveau de protection. Mais réussir ce tournant stratégique demande d'abord de bien saisir le problème de la sécurité des données digitales.

Les 3 dimensions de la sécurité

De quoi parle-t-on lorsque l'on aborde le sujet de la sécurité des données RH ? Si le sens du terme sécurité semble intuitif, il recouvre en réalité trois dimensions bien distinctes qu'il importe de distinguer clairement.

1. La sécurité physique

Des données sécurisées sont avant tout des données dont les supports sont protégés contre les risques physiques : incendie, destruction volontaire, perte, etc. Les données sont désormais l'une des principales richesses des entreprises et pour beaucoup d'entre elles, une perte importante de données peut signifier la disparition à très court terme.

> *Pour les responsables des ressources humaines, les données constituent un outil de travail à part entière. Une menace à leur intégrité représente une menace pour la continuité du service RH. C'est pourquoi DRH et DSI doivent collaborer assurer une disponibilité permanente et un niveau de service constant.*

> *« La base de données sociales, qui est le fondement d'une solution de paie, constitue un gisement d'informations pertinentes pour piloter nos ressources humaines et améliorer le profilage de nos futurs embauchés. Encore faut-il disposer des capacités de traitement de ces données. »*

Guillaume Beghin,
Directeur des ressources humaines,
Legendre

* Étude BPI France

2. La protection contre les intrusions

C'est le risque le mieux connu des entreprises et pour cause : selon le baromètre du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) publié en 2018, 8 entreprises françaises sur 10 ont déjà fait l'objet d'une cyber-attaque. La plupart du temps, ces attaques entraînent des pertes financières directes : interruption forcée de l'activité, atteinte à la réputation, paiement de pénalités aux clients ou encore condamnations légales.

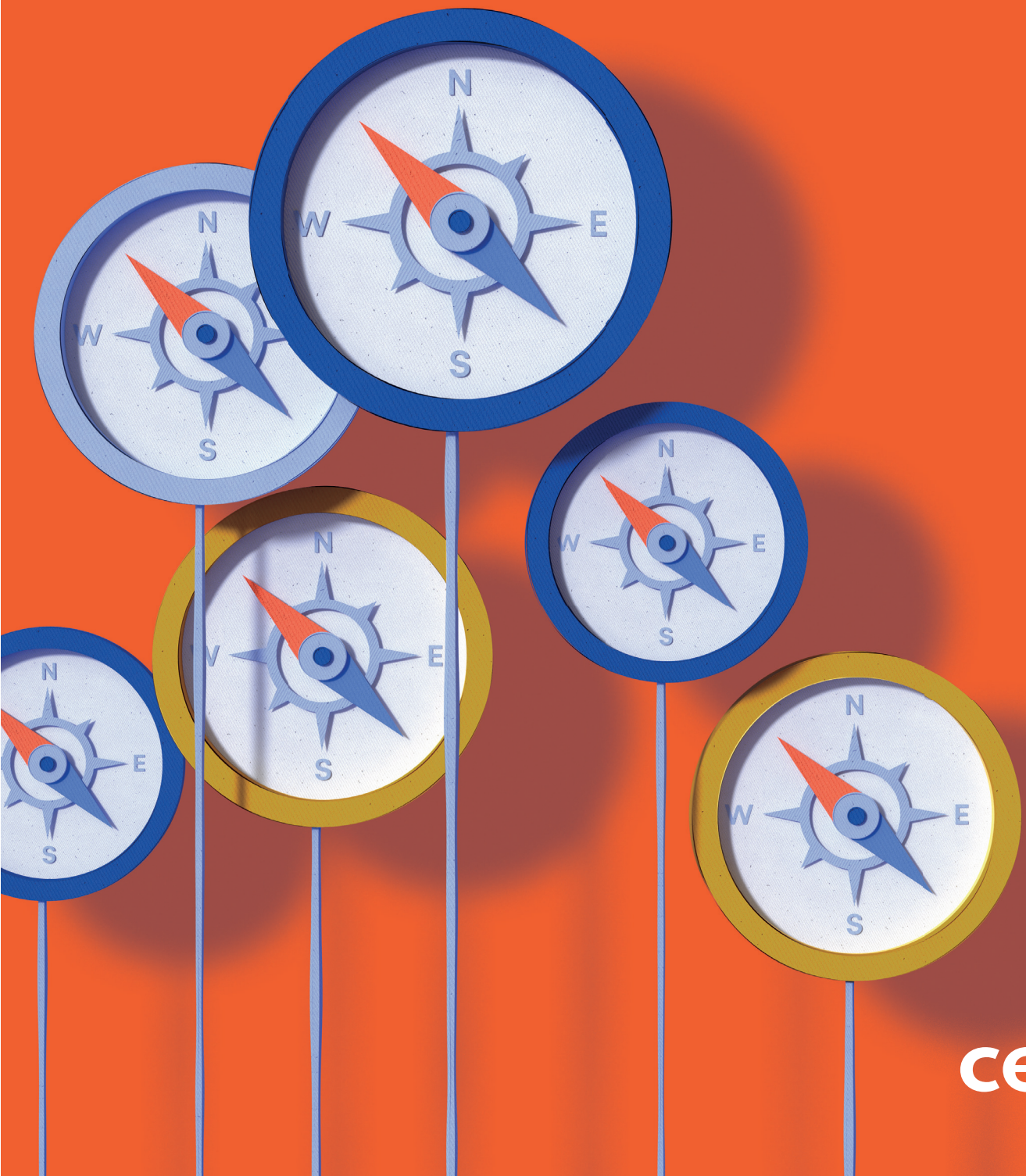
› *La plupart des intrusions sont dues à des erreurs humaines en interne, comme un clic imprudent sur une page de phishing ou une négligence technique. Pour les prévenir, les ressources humaines et la DSI doivent assumer un rôle de sensibilisation et de prévention en matière de comportement digital des salariés : gestion des mots de passe, vérifications de base des sites web, etc.*

3. La confidentialité

La confidentialité des données a longtemps été le parent pauvre de la sécurité. Si les intrusions étaient un risque bien identifié, la possibilité d'une diffusion par négligence de données personnelles était sous-estimée. En dehors de certaines données sensibles, peu de mesures sérieuses étaient alors mises en œuvre pour la faire respecter. Mais les évolutions réglementaires récentes et notamment le RGPD ont complètement rebattu les cartes : la confidentialité est désormais prise au sérieux par les entreprises et, de plus en plus, par leurs salariés.

› *Le rôle des services RH dans cette prise de conscience est central. Pour protéger la confidentialité des nombreuses données personnelles sensibles dont ils ont la responsabilité, les responsables RH doivent accompagner et sensibiliser leurs collaborateurs.*

Explorer toujours



cegid

La révolution Cloud

Le Cloud a transformé le monde des applications professionnelles et les outils RH n'échappent à ce mouvement de fond. Cette disruption technologique a notamment eu un impact considérable sur l'ensemble des questions de sécurité des données, qu'elles concernent la sécurité physique, la confidentialité ou la protection contre les intrusions.

L'On-Premise : le modèle du chacun pour soi

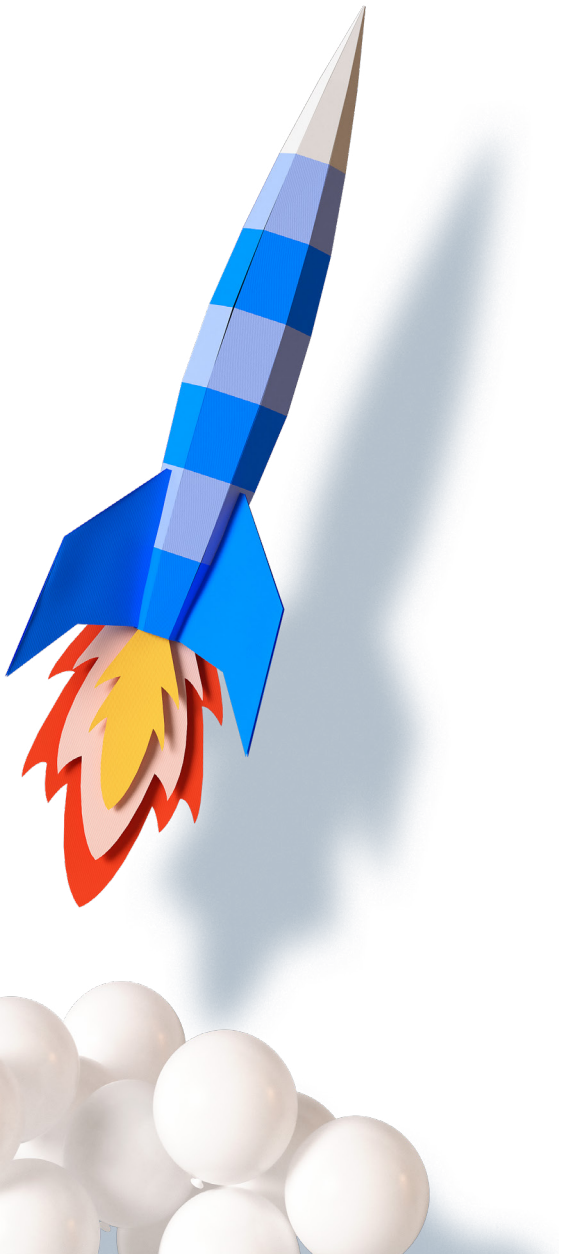
L'informatique d'entreprise a longtemps été dominée par les systèmes On-Premise : des systèmes hébergés et gérés par l'entreprise elle-même et donc entièrement sous le contrôle de la DSI. Celle-ci était alors responsable de l'ensemble des questions de sécurité et devait les prendre en charge avec ses propres moyens techniques et humains. Une situation qui engendrait d'importantes inégalités entre petites et grandes entreprises.

Vers la mutualisation des ressources

Aujourd'hui, le Cloud, et en particulier les applications en SaaS, représente une part importante de l'écosystème applicatif des entreprises de toute taille : en effet, plus de 50% des applications installées dans des domaines aussi divers que le marketing, les réseaux sociaux d'entreprise ou le partage de fichiers, sont délivrées en Cloud*.

En matière de protection, le SaaS constitue un moyen idéal pour les entreprises de mutualiser leurs ressources et ainsi d'avoir toutes accès au même niveau de sécurité.

Mais le niveau de sécurité offert par le Cloud est-il réellement supérieur à celui que l'on pourrait attendre d'une infrastructure privée ? C'est la question à laquelle nous allons répondre en examinant les trois dimensions de la sécurité dans une infrastructure cloud.



* Étude IDC France 2017

La sécurité physique dans le Cloud

Des infrastructures à toute épreuve

Lorsque des responsables de paie utilisent une application SaaS, les données RH qu'ils traitent sont stockées sur les infrastructures de leur fournisseur Cloud. Ces données bénéficient donc des mesures de sécurité drastiques qui s'appliquent aux data centers.

Une architecture résiliente sans *single point of failure*

Les data centers sont conçus pour être des systèmes hautement résilients. Tous les éléments qui les composent (composants, câbles, logiciels, données, etc.) sont doublés pour prévenir tout risque de panne. Aucun point précis du réseau ne doit être indispensable et potentiellement responsable d'une défaillance, c'est le principe d'une architecture sans single point of failure.

Des sauvegardes multisites pour prévenir les pertes

Si les données sont doublées au sein d'un même data center, elles sont également sauvegardées chaque jour sur plusieurs sites différents. Seule une défaillance physique simultanée des équipements de plusieurs data centers pourraient donc mettre leur intégrité en péril.

Une surveillance constante

Les data centers sont de véritables bunkers faisant l'objet d'une surveillance permanente. Les accès sont contrôlés par des systèmes de badge et de reconnaissance biométrique tandis que les visiteurs sont accompagnés à tout instant par des employés formés à la sécurité.

Une prévention active des incendies

Les serveurs dégagent de la chaleur, les data centers doivent donc être refroidis en permanence et protégés des incendies. Des systèmes innovants de refroidissement à air, à eau et désormais à huile sont donc utilisés pour maintenir chaque serveur à une température constante. Les installations sont inspectées régulièrement et en profondeur et sont équipées de systèmes d'alerte extrêmement sensibles pouvant détecter immédiatement le foyer d'un éventuel incendie.

Protection contre les intrusions

Des équipes d'experts au service de tous

Les compétences en cyber-informatique sont au cœur d'une course aux talents effrénée qui voit un grand nombre d'entreprises tenter d'attirer de trop rares administrateurs réseau et système en faisant monter les enchères salariales et en améliorant leur expérience collaborateur. Mais toutes les entreprises ne peuvent se permettre de jouer à ce jeu. C'est pourquoi beaucoup se tournent vers le cloud et ses data centers hypersécurisés. Ceux-ci sont en effet protégés des intrusions par des procédés innovants. Voici quelques-uns des systèmes de protection mis en place sur les infrastructures Cegid :

- ***Solution antivirus et antimalware centralisée***
- ***Identification et traçage de l'ensemble des connexions***
- ***Chiffrage de l'ensemble des données via des protocoles sécurisés lorsqu'elles transitent sur le réseau***
- ***Pare-feux et sondes de sécurité IPS pour analyser le trafic, détecter et prévenir toute intrusion***

En faisant appel à un prestataire cloud, les entreprises de toute taille bénéficient donc d'une solution complète de cybersécurité sans aucun investissement de long terme. La mutualisation des coûts les dispense ainsi simultanément des coûts matériels et salariaux, des frais liés à l'entretien des infrastructures comme à la formation de responsables de la sécurité. Leurs salariés peuvent ainsi se concentrer sur leur cœur de métier et confier leurs données à des spécialistes.

Pour assurer cette sérénité à leurs collaborateurs, les équipes internes de la DRH et de la DSI ont un rôle crucial à jouer. Elles doivent s'allier pour concevoir des processus de travail sécurisés. En effet, des outils parfaitement sûrs restent vulnérables s'ils ne sont pas utilisés et gérés de façon adaptée. Campagnes de prévention contre le phishing, définition précise et suivi régulier des droits d'accès, sensibilisation à la question des mots de passe sécurisés, sont autant de sujets techniques impliquant nécessairement spécialistes des systèmes d'informations et responsables des ressources humaines.

> *« L'exploitation de Cegid HR Ultimate en mode SaaS, nous dispense d'investissements coûteux en hébergement et en maintenance. Elle nous donne également la possibilité de déléguer à Cegid la responsabilité de la conformité sociale et réglementaire. »*

Guillaume Beghin,
Directeur des ressources humaines,
Legendre

RGPD

Le tournant de la confidentialité dans le Cloud

Longtemps ignorée, méconnue ou sous-estimée, la confidentialité des données personnelles est devenue un enjeu majeur avec l'entrée en vigueur le 25 mai 2018 du Règlement Général sur la Protection des Données (RGPD). Texte de référence sur la protection des données personnelles en Union Européenne, il impose des précautions strictes dans leur traitement et des amendes lourdes en cas de négligence ou de responsabilité directe dans une fuite de données.

Une coresponsabilité entre l'entreprise et son fournisseur cloud

Pour les fournisseurs cloud, le RGPD a été un tournant complet de leur action en matière de confidentialité. L'article 26 du règlement impose une « coresponsabilité » entre l'entreprise et ses sous-traitants, parmi lesquels les fournisseurs de logiciels et hébergeurs de données sont particulièrement concernés. Ces derniers doivent donc veiller à ce que les données aient été recueillies avec le consentement « explicite » des utilisateurs, mettre en place des processus de sécurité et aider leurs clients à se mettre en conformité avec le règlement.

Un règlement impopulaire devenu un atout du cloud européen

D'abord mal perçu et contesté par les entreprises, ce règlement européen s'est en réalité transformé en un réel atout pour l'ensemble des sociétés européennes dont l'activité implique de traiter des données personnelles. En obligeant clients et fournisseurs cloud à travailler main dans la main pour une confidentialité totale des données, il a créé un espace de confiance en Union Européenne, véritable argument marketing qui suscite l'intérêt du monde entier.

Le risque du « Shadow IT »

Selon le RGPD, le chef d'entreprise est responsable des traitements appliqués à l'ensemble des données personnelles collectées par ses services. Il doit donc s'assurer des garanties apportées par ses sous-traitants en matière de protection des données. Mais comment faire s'il ne sait pas quels services sont utilisés par ses équipes ? C'est tout le problème du « shadow IT » : des services cloud utilisés par les métiers sans l'aval de la DSI et qui peuvent compromettre des données sensibles. Le respect du RGPD implique donc une chasse à ces services cloud clandestins.

Optimiser la sécurité des processus internes

Les services Cloud ont transformé la façon qu'avaient les entreprises d'appréhender la sécurité en leur permettant de mutualiser les ressources. Mais le Cloud n'est pas synonyme d'externalisation complète des questions de sécurité. La confidentialité de données hébergées sur des serveurs sécurisés peut être compromise par un simple processus interne défaillant.

C'est pourquoi une digitalisation réussie ne passe pas que par des choix technologiques mais aussi par une remise à plat complète des processus internes visant à optimiser leur sécurité.

Mener à bien ce véritable défi organisation demande d'organiser ses efforts autour de trois étapes principales :

1. Sensibiliser les salariés
2. Adopter l'approche « privacy by design »
3. Choisir les bons outils

Sensibiliser les salariés

Comme tout projet d'entreprise global, la digitalisation doit passer par une mobilisation des salariés et une communication interne fédératrice. La sensibilisation à la question de la sécurité des données doit, dès le départ, être incluse dans cet effort de communication. La sécurité est en effet en jeu dans chaque tâche des salariés et doit donc faire l'objet de formations et d'initiatives d'information spécifiques.

Rédiger une charte informatique

Pour faire prendre conscience à chacun des risques liés à l'usage des outils numériques, une charte informatique peut être rédigée. Pour lui donner une plus forte portée et une valeur contraignante il est conseillé de l'adosser au règlement interne de l'entreprise.

Cette charte doit notamment inclure :

- Les règles d'utilisation de l'ensemble des outils et matériels fournis par l'entreprise
- Les procédures à appliquer en cas de fuite d'information avérée ou potentielle
- Les sanctions applicables en cas de manquement aux règles de sécurité

Organiser des séances de formation dédiées

Les séances de formation en présentiel sont le meilleur moyen d'attirer efficacement l'attention des salariés sur les questions de sécurité. Elles sont l'occasion pour eux de se remettre en question et de réaliser des exercices pratiques.

Faire signer des engagements individuels

La signature d'engagements individuels spécifiquement dédiés à la question de la sécurité des données est une initiative plus engageante que la simple inclusion d'une charte informatique dans le règlement intérieur. Ces engagements individuels sont destinés en priorité aux personnes manipulant des données à caractère personnel dans leurs tâches quotidiennes mais peuvent être élargis à l'ensemble des salariés ayant accès à des outils informatiques.

Adopter l'approche « privacy by design »

Longtemps, les entreprises ont développé des services sans prendre en compte la question de la confidentialité et ne les ont sécurisés qu'ultérieurement, au gré des évolutions réglementaires. Face aux risques financiers, opérationnels et réglementaires, elles ne peuvent plus se permettre d'adopter une telle approche. Elles doivent désormais adopter une approche « privacy par design », c'est-à-dire développer des services prenant en compte la question de la confidentialité des données dès leur phase de conception.

Un principe structurant

L'approche « privacy by design » implique d'aborder la question de la confidentialité et de la sécurité en général à chaque étape de développement d'un produit, à chaque réunion importante pouvant avoir un impact sur le traitement de données personnelles

> *Cette approche demande donc une coopération renforcée entre les équipes métier et les équipes informatiques qui doivent être consultées sur les implications en matière de confidentialité et de protection contre les intrusions de chaque nouvelle fonctionnalité.*

Authentifier les utilisateurs

Le meilleur moyen de le mettre en place au sein de l'entreprise et dans les services qu'elle fournit est d'utiliser des outils intégrant une gestion fine des accès. Chaque utilisateur est ainsi authentifié et associé à un certain nombre de droits de consultation en fonction des informations qui peuvent être partagées avec lui.

Une approche transverse

L'approche « privacy par design » nécessite une collaboration étroite entre DSI et DRH. Lors de la conception d'un projet, la confidentialité doit en effet être abordée d'un point de vue technique comme du point de vue des processus RH.

Choisir les bons outils

Lorsque les salariés ont été sensibilisés à la question de la sécurité des données et que leurs processus ont été entièrement revus au prisme de la confidentialité, il ne reste plus aux entreprises qu'à leur fournir les outils adéquats pour maintenir le niveau de sécurité fixé.

Les coffres-forts électroniques

Selon la réglementation, les données personnelles utilisées par les services RH ne cessent jamais d'appartenir aux salariés concernés. C'est donc logiquement que de plus en plus d'entreprises placent l'ensemble des données RH de chaque salarié dans un coffre-fort électronique individuel donc la clé reste sa propriété exclusive même après son départ de l'entreprise.

Les clés USB cryptées

Dans le cas où des données sensibles devraient être transportées ou communiquées sur un périphérique mobile, les clés USB cryptées sont à privilégier. Celles-ci contiennent un générateur de numéros aléatoires produisant une clé de cryptage uniquement accessible avec un mot de passe. La performance d'un cryptage matériel est supérieure à celle d'un cryptage logiciel traditionnel car ce n'est pas le système hôte qui prend en charge les opérations de cryptage et décryptage mais bien le support mobile.

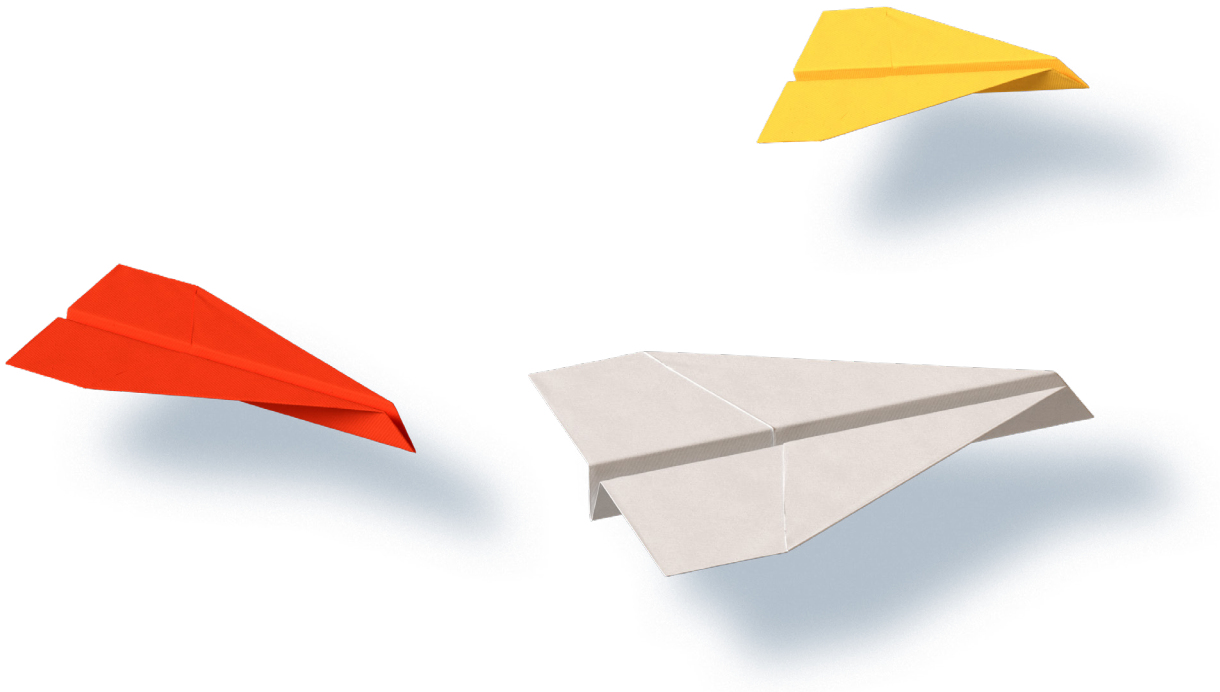
Privilégier le made in France

Choisir des services dont les data centers sont situés sur le territoire français présente plusieurs avantages. Cela permet notamment de s'assurer que les données traitées par le service sont hébergées selon les normes et réglementations en vigueur en France. C'est également un moyen de favoriser la coopération entre les équipes techniques de l'entreprise et celles de son prestataire en cas de défaillance ou de fuite de données.

Conclusion

A l'heure où la sécurité et la confidentialité des données deviennent des préoccupations majeures pour les salariés comme pour le législateur, les services RH doivent avoir une approche globale de ces questions et un contrôle intégral de leurs processus. Sécurité physique, protection contre les intrusions et confidentialité doivent être assurées de façon complémentaire par une attention aux processus internes comme aux prestations externes.

Seule une telle approche globale peut permettre aux responsables RH de définir précisément les droits de consultation de toutes les données traitées par son service. Un niveau de contrôle et de protection de la vie privée que ne peuvent atteindre les systèmes reposant totalement ou partiellement sur le papier. Loin d'être un risque, la digitalisation est dans cette optique une opportunité pour faire face aux obligations légales et morales qui lient les entreprises à leurs salariés.



S’inspirer de nos clients

cegid

À propos de Cegid :

Cegid est un acteur majeur des solutions de gestion pour les professionnels des métiers de la Comptabilité, de la Finance et de la Fiscalité, de la Paie et des Ressources Humaines et du Retail. Fort de son expérience de leader des solutions de gestion SaaS, Cegid accompagne la digitalisation des entreprises et des organisations publiques. Cegid combine une vision prospective et pragmatique des métiers, et la maitrise des nouvelles technologies afin d'apporter de l'innovation utile. Avec une maitrise unique du réglementaire. Cegid s'engage dans la durée avec ses clients.

Dans un monde en évolution rapide, Cegid ouvre les possibles et permet à chaque métier d'augmenter sa valeur ajoutée. Cegid compte 2400 collaborateurs et vend ses solutions dans 75 pays. Cegid a réalisé un chiffre d'affaires de 401 M€ en 2018. Pascal Houillon est le Directeur Général depuis mars 2017.

cegid

Siège social
Cegid Group - 52 quai Paul Sédallian
69 279 Lyon Cedex 09

Tél. 0 811 884 888

Société par Actions Simplifée au capital de 18 606 860 euros - SIREN 410 218 010 RCS LYON - SIRET 410 218 010 00032 - TVA CEE FR 07 410 218 010

www.cegid.com

Cegid - Juillet 2019