arcserve®

LIVRE BLANC

Gestion des données en conformité avec le Règlement général sur la protection des données (GDPR)

Par Christophe Bertrand, Vice-Président Produit Marketing

Traditionnellement, les données à caractère personnel telles que le nom, l'adresse, le numéro de téléphone, la date de naissance, le sexe, l'âge et l'origine ethnique étaient recueillies avec l'accord des personnes concernées lorsqu'elles remplissaient des formulaires, effectuaient des réservations de vacances, achetaient des billets et participaient à des compétitions. Mais avec l'évolution des réseaux sociaux, des Smartphones et des applications en nuage, les informations d'identification personnelles (IIP) peuvent être recueillies de manière beaucoup plus indirecte. Par exemple, votre adresse IP et votre emplacement peuvent être capturés à partir de votre téléphone pendant une pause-café.

Trop souvent, les personnes ont peu ou pas conscience de l'étendue et de l'ampleur de la collecte, de l'analyse et de la communication de leurs données. Finalement, l'association explosive de la collecte des données à caractère personnel sans cesse croissante et de la forte augmentation des incidents concernant la perte des données a conduit à la création d'un nouveau règlement solide destiné à protéger les données à caractère personnel.

En raison de l'augmentation rapide des capacités technologiques et de l'absence des frontières de l'économie numérique moderne, les gouvernements ont dû s'adapter pour apporter une meilleure protection des données et améliorer les droits fondamentaux des personnes concernées. Le 25 mai 2018, le règlement sur la protection des données le plus radical au monde, le Règlement général sur la protection des données (General Data Protection Regulation / GDPR) de l'Union Européenne, deviendra une loi.

Le GDPR donne aux résidents de l'UE le droit de prendre connaissance des données les concernant stockées par les entreprises, de retirer leur consentement quant à leur utilisation, et d'exiger leur destruction immédiate. Selon l'article 12 du GDPR, cette demande doit être gratuite, facile à réaliser et doit être satisfaite sans « délai injustifié et au plus tard dans un délai d'un mois ».

Le règlement vise à harmoniser le fonctionnement des 28 États membres de l'UE et à encourager les entreprises à assumer leurs responsabilités, à être plus transparentes et à garantir la sécurité des données qu'elles détiennent. Toute entité qui stocke ou traite les données à caractère personnel des résidents de l'UE sera tenue de respecter cette nouvelle loi, quel que soit l'endroit du siège de cette entreprise. De plus, il donne la possibilité aux résidents de l'UE de contrôler les données les concernant détenues par une entreprise.

L'UE a donné aux entreprises jusqu'en mai 2018 pour appliquer les dispositions de cette nouvelle loi. En effet, la mise en œuvre des processus et des capacités exigés par le GDPR demande du temps et nécessite des investissements importants par les entreprises. Compte tenu de la portée et de la transformation qui va découler du GDPR, il est important que les entreprises examinent leur façon de traiter les données à caractère personnel.

Le non-respect entraînera des amendes allant jusqu'à 4 % du chiffre d'affaires global ou 20 millions d'euros, selon le chiffre le plus élevé des deux. En réalité, l'équation a été modifiée - au lieu de choisir de simplement payer des amendes et ne pas respecter la réglementation, les entreprises doivent à présent investir dans la préparation à l'application des dispositions du GDPR ou être soumises à des amendes conséquentes.

Le GDPR impose une réforme globale et une action rapide, dont les principales exigences doivent être respectées :

- Responsabilité et gouvernance - Maintenir les registres appropriés sur les activités de traitement des données et mettre en place des mesures qui démontrent le respect de la réglementation, telles que des audits.
- Notification d'une violation - L'entreprise doit obligatoirement signaler une violation à l'autorité de contrôle concernée dans les 72 heures après en avoir pris connaissance.
- Limitation relative au stockage - Les données à caractère personnel doivent être conservées uniquement le temps nécessaire à l'accomplissement de l'objectif qui était poursuivi lors de leur collecte.
- Droits des personnes physiques - Une personne physique peut demander la suppression ou le retrait des données à caractère personnel lorsqu'il n'existe aucune raison suffisante à leur existence à plus long terme.

Arcserve attire particulièrement l'attention, parmi ces exigences, sur la nécessité de protéger les données et de prévenir la perte des données. Les infrastructures informatiques doivent tirer parti de la technologie de pointe pour éviter les situations impliquant la perte de données.

À ce jour, il n'existe pas de solution unique qui permettrait de satisfaire tous les aspects du GDPR. De nombreuses facettes différentes affectent les processus informatiques et liés aux données, y compris la sauvegarde et l'archivage.

Conséquences pour la sauvegarde et l'archivage

L'article 5 du GDPR énonce les principes majeurs relatifs à la protection des données et décrit comment les entreprises doivent traiter les données à caractère personnel, comment elles peuvent être stockées et comment elles doivent être sauvegardées. L'article 5 stipule que les entreprises peuvent conserver des copies de sauvegarde et d'archives des données si elles sont traitées de manière à assurer une sécurité appropriée des données à caractère personnel.

L'article 5 du GDPR exige que les données à caractère personnel soient :

a) traitées de manière licite, juste et transparente au regard de la personne concernée ;

b) recueillies pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré comme incompatible avec les finalités initiales ;

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;

d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, en relation avec les finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées au plus vite ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le GDPR afin de garantir les droits et libertés de la personne concernée ;

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Le GDPR comprend des dispositions qui favorisent la responsabilité et la gouvernance. Elles complètent les exigences relatives à la protection des données du GDPR. Le nouveau principe de responsabilité énoncé à l'article 5 (2) exige que les entreprises démontrent qu'elles sont en mesure de respecter les principes et déclarent explicitement qu'elles sont responsables de leur respect.

a) Mettre en œuvre des mesures techniques et organisationnelles appropriées qui garantissent et démontrent le respect par l'entreprise.

b) Tenir un registre approprié des activités de traitement.

c) Le cas échéant, nommer un responsable de la protection des données.

d) Mettre en œuvre des mesures qui respectent les principes de protection des données dès la conception et de protection des données par défaut.

e) Utiliser des études d'impact sur la protection des données, le cas échéant.

Arcserve répond aux exigences du GDPR de façon unique

Le GDPR demande à ce que la gouvernance des données soit améliorée pour la sauvegarde et l'archivage. Les produits de sauvegarde et d'archivage existants sont destinés à résoudre les difficultés de la gestion individuelle des données, donc n'ont pas la capacité de fournir une solution globale conforme au GDPR. Arcserve a adopté une approche unique pour fournir un ensemble solide de produits répondant aux besoins des exigences plus générales du GDPR.

Il existe un processus expansif qui est nécessaire pour définir ce qui constitue des données à caractère personnel dans votre entreprise. Il est logiquement présent dans les bases de données, les courriers électroniques et les postes de travail. Les données à caractère personnel sont définies assez largement pour inclure les courriers électroniques personnels, les adresses de courrier électronique et les autres données qu'une entreprise peut recueillir non seulement dans le cadre de ses activités de marketing et activités commerciales, mais aussi dans le cadre d'un processus normal de sauvegarde et de protection des données. Le GDPR exige le consentement des propriétaires des données au moment de leur collecte. En substance, les copies de sauvegarde et les courriers électroniques contiennent des données à caractère personnel qui ajoutent un fardeau supplémentaire: les entreprises doivent gérer toutes les copies de sauvegarde et les archives de courriers électroniques conformément aux exigences du GDPR. Des copies de sauvegarde sont effectuées pour conserver des données sauvegardées hors site en cas de sinistre. Les entreprises peuvent fréquemment avoir une douzaine, ou plus, de copies de chaque sauvegarde.

Lorsque les entreprises conservent des données sauvegardées d'habitants de l'Union Européenne, la sauvegarde doit se trouver dans l'Union européenne, ainsi que les copies des sauvegardes, les sauvegardes sur bande ou les copies en nuage, sauf si vous avez un système donnant la possibilité au client de vous autoriser à les conserver en dehors de l'UE.

Les entreprises qui maintiennent des archives de courriers électroniques doivent accorder une attention particulière aux exigences du GDPR. Il est fréquent que les courriers électroniques soient archivés et conservés pendant des années en raison des exigences imposées à l'entreprise, des exigences réglementaires et des exigences de conservation à des fins juridiques. Dans le cas où un utilisateur retire son consentement, un administrateur a besoin des outils standards fournis par la solution d'archivage pour identifier les courriers électroniques et les supprimer des archives. Les registres des activités sont nécessaires pour conserver une trace de la destruction comme preuve pour les audits.

Avec la technologie de sauvegarde actuelle, il est impossible de supprimer les données à caractère personnel des sauvegardes, quel que soit le fournisseur.

- Cela intensifierait également le risque de fraude massive s'il est possible de faire facilement «disparaître» une personne physique de toutes les données directes et des données des archives / des sauvegardes.
- Cela entrerait en conflit avec les règles relatives à la conformité qui favorisent la conservation et/ou l'immutabilité des données.

Vous êtes autorisé à conserver les données à caractère personnel dans vos sauvegardes, même si la personne concernée a exercé son droit d'être oubliée. MAIS... vous n'êtes pas autorisé à effectuer une restauration de ces données (à moins d'un motif juridique, comme un procès).

- Conformément au GDPR, les données à caractère personnel stockées sur des copies de sauvegarde sont marquées comme étant éliminées et ne peuvent pas être restaurées une fois qu'un utilisateur retire son consentement.
- Si vous devez effectuer une restauration qui inclut des données à caractère personnel devant être oubliées, alors vous devriez les effacer.
- Il existe un consensus sur le fait que le droit d'être oublié s'applique aux données de production / actuelles et non aux archives ou aux sauvegardes

Les données en général, y compris les sauvegardes, doivent être protégées contre toute violation (le cryptage par exemple). Les solutions d'Arcserve ont de telles capacités.

Si vous conservez des données qui sont considérées comme des données à caractère personnel ou sensible, telles que les données de clients, alors les données des citoyens de l'Union Européenne (la sauvegarde) devraient se trouver dans l'Union Européenne (localisation).

Il est juste de dire qu'à ce stade, le GDPR crée un certain nombre de zones d'ombre pour les entreprises et les fournisseurs. Les interprétations et la jurisprudence permettront de les éclaircir à l'avenir au fur et à mesure de sa mise en œuvre.

Arcserve Unified Data Protection (UDP)

Arcserve offre des capacités de protection des données de qualité professionnelle sans la complexité souvent associée aux solutions de protection des données destinées aux entreprises. Les petites équipes informatiques, souvent débordées, peuvent facilement sauvegarder les données en nuage, virtuelles et physiques, en les protégeant de et contre n'importe quelle cible, tout en configurant et en gérant tous les aspects de la protection des données grâce à une console d'utilisateur unique, simple et élégante. Au fur et à mesure que les besoins des entreprises changent ou que les exigences évoluent, les équipes informatiques deviennent facilement performantes sans mises à niveau lourdes ou ajouts de solutions supplémentaires.

Une exigence clé du GDPR, comme l'indique l'article 5 (2) énonce que « le responsable du traitement assume la responsabilité et doit être en mesure de démontrer le respect des principes ».

Du point de vue du respect du règlement, des tests de sauvegarde et de récupération réguliers, ainsi que la réalisation de rapports sur la protection des données, sont des bons moyens de démontrer à votre Responsable de la protection des données (nouvelle fonction) que vous êtes en conformité et protégez vos données de manière efficace.

Arcserve UDP permet de :

- Documenter la sécurité des données, y compris la fréquence à laquelle les données sont protégées et la durée nécessaire pour restaurer une copie de sauvegarde, grâce aux rapports sur les contrats de prestation de services (SLA) et Assured Recovery.
- Documenter la sauvegarde, quelles données sont protégées ainsi que l'emplacement où les données sont stockées, grâce à des rapports standards.
- Documenter la durée de conservation des copies de sauvegarde et à quel moment elles sont détruites grâce aux rapports relatifs à la politique de conservation.

Avantages d'Arcserve UDP

Amélioration de la protection, de la récupération et de la disponibilité des données

- Architecture unifiée autour de technologies de protection des données de base à l'aide d'une console unique.
- Une solution riche en fonctionnalités prenant en charge une grande variété d'environnements.
- Des plans de protection personnalisés pour répondre à des besoins spécifiques en matière de protection des données.
- Rapports avancés pour démontrer le respect des principes du GDPR.

Amélioration de l'efficacité opérationnelle

- Plus grande efficacité de l'administrateur grâce à la console de gestion unifiée d'Arcserve
- La facilité d'utilisation et les capacités étendues permettent d'économiser le temps et d'augmenter la valeur
- Atténuation de la consommation des ressources réseau et de stockage

Amélioration des capacités à démontrer le respect des principes du GDPR

- Le cryptage protège les copies de sauvegarde pour sauvegarder les données conformément aux exigences du GDPR.
- Les options de récupération flexibles permettent de gérer les copies de sauvegarde conformément aux exigences du GDPR.
- Les options de conservation permettent la conservation à long terme, la conservation à des fins juridiques et l'élimination des données justifiable.
- Capacité de tester, de mesurer et de déclarer les processus de récupération afin d'être en accord avec les exigences du GDPR

Arcserve UDP Archiving

Arcserve UDP Archiving permet aux entreprises de relever facilement les défis associés à la recherche de courriers électroniques, à la conformité et aux risques juridiques grâce à une solution spécifique qui prend en charge les déploiements sur site, en nuage privés et publics. Les petites équipes informatiques, souvent débordées, optimisent l'efficacité opérationnelle et réduisent les coûts en configurant et en gérant tous les aspects de leurs stratégies de protection et d'archivage des données grâce à une console d'utilisateur unique, simple et élégante.

La technologie de messagerie électronique, nouvelle solution d'Arcserve UDP, apporte tous les outils pour aider les utilisateurs à gérer les courriers électroniques archivés afin de respecter les exigences du GDPR. Elle prend en charge une architecture multi-utilisateurs, permettant aux entreprises multinationales et décentralisées de séparer les archives de courriers électroniques en fonction du site, de la division ou du département. Par exemple, un courrier électronique créé dans un pays européen peut être géré et stocké séparément des courriers électroniques d'origine nord-américaine.

Arcserve UDP Archiving est une solution d'archivage de courriers électroniques spécialement conçue pour gérer les courriers électroniques de manière à respecter la règlementation telle que le GDPR, et offre plusieurs contrôles standards pour répondre rapidement aux demandes de retrait du GDPR. La solution d'archivage UDP peut également aider à démontrer la suppression des données à caractère personnel des archives.

Lorsque les personnes physiques retirent leur consentement, les administrateurs utilisent des outils intégrés de eDiscovery pour rechercher, identifier et supprimer rapidement tous les courriers électroniques envoyés ou reçus par la personne concernée. Les administrateurs ont accès à des registres d'archivage détaillés qui énumèrent toutes les actions effectuées et disposent d'une preuve de destruction. Souvenez-vous que cela doit être effectué en accord avec les exigences de conformité. Le GDPR n'est pas véritablement clair à ce sujet.

Arcserve UDP Archiving Avantages en un coup d'œil

Administration à l'aide d'une console unique pour l'archivage, la recherche et la conservation.

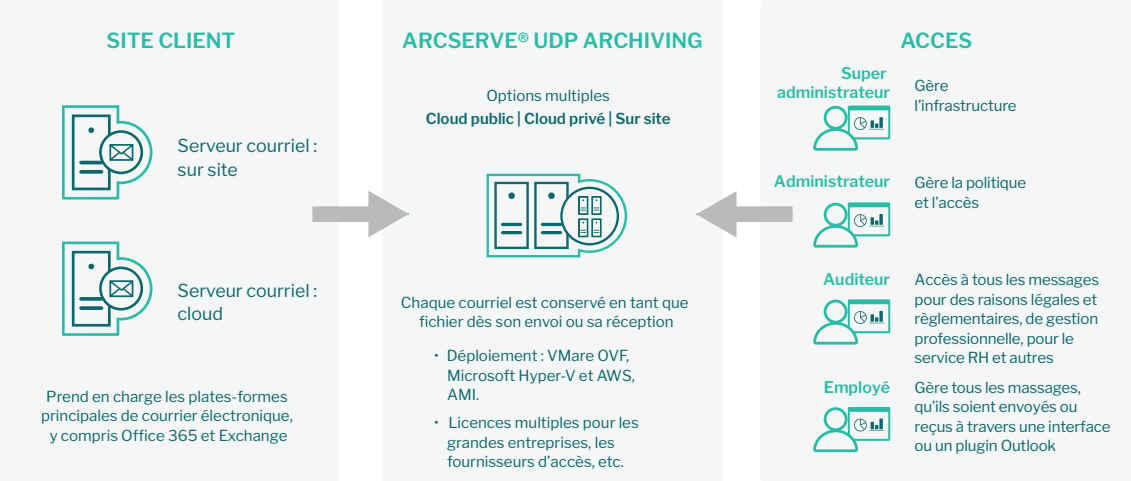
Contrôle multi-utilisateurs par département, division ou site.

Recherche rapide et efficace, suppression des courriers électroniques archivés

Pas de limite sur le nombre de boîtes aux lettres par recherche.

Rapports basés sur les registres d'activités, constituant des preuves de destruction

Topologie de Arcserve UDP Archiving



Conclusion

Le GDPR accorde aux résidents de l'UE le droit de retirer leur consentement, d'exiger la destruction de leur courrier électronique et d'autres données à caractère personnel, entraînant l'émergence de nouvelles exigences de conformité que les entreprises doivent respecter. Bien que le droit de supprimer des données à caractère personnel ait été souligné par beaucoup, il ne s'agit que de l'un des aspects du règlement. Il est également clairement axé sur la protection des données à caractère personnel, ce qui affecte les décisions opérationnelles liées à la sauvegarde et à la récupération.

Les équipes chargées de la gestion des données sauvegardées et des données de messagerie ont besoin d'outils solides et faciles à utiliser qui leur permettent d'identifier rapidement les données à caractère personnel et de les supprimer de leurs systèmes. Arcserve UDP et sa solution d'archivage apportent les capacités nécessaires pour démontrer le respect des principes du GDPR, y compris la sauvegarde et la récupération à partir d'une console centrale, une récupération granulaire avec la possibilité d'exclure des fichiers, le suivi et les rapports sur l'ensemble des activités pour démontrer le respect de la réglementation.

Dans le cas où un utilisateur retire son consentement, un administrateur peut rapidement identifier et supprimer les courriers électroniques personnels archivés à l'aide d'outils standards, assurant ainsi le respect du GDPR et évitant les éventuelles sanctions et amendes. Arcserve UDP et sa solution d'archivage constituent des éléments majeurs pour permettre la mise en œuvre d'une stratégie solide visant à assurer le respect des exigences du GDPR.

Pour plus d'informations sur Arcserve, **veuillez consulter** arcserve.com