BOMGAR

COMPRENDRE LE RGPD ET S'Y PRÉPARER

Le paysage de l'information a beaucoup changé depuis l'introduction par l'Union européenne en 1995[1] de sa Directive sur la Protection des Données visant à préserver la vie privée des citoyens de l'UE. Les quantités, les sources et les types de données que les entreprises peuvent collecter et exploiter n'ont cessé de se multiplier à un rythme exponentiel, tout comme la valeur qu'elles représentent pour les entreprises qui les exploitent.

Avec l'émergence de la culture du « toujours connecté », sous l'effet des nouvelles capacités des appareils mobiles et de la transformation numérique des services, les entreprises sont désormais en mesure de réunir et de traiter un large panel de données personnelles et comportementales à chacune de nos interactions en ligne. De plus, des entreprises comme Facebook et Google collectent chaque jour des quantités impressionnantes de données au point qu'un récent article de la BBC[2] indique que l'ampleur des données collectées par Facebook en fait l'une des entreprises les plus influentes du monde.

Dans le même temps, le stockage et le traitement de ces données ont quitté le périmètre informatique traditionnel et les salles de serveurs pour les environnements cloud et hybrides de data centers implantés partout dans le monde. La façon dont les entreprises traitent les données évolue également maintenant que la confidentialité des données est menacée. La dernière édition du Secure Access Threat Report[3] de Bomgar révèle que 57% des salariés des entreprises sondées envoient des fichiers à des comptes e-mail personnels, que 55% téléchargent des données sur une clé ou un disque dur externe et que les salariés de 53% des entreprises se connectent au réseau interne à partir de connexions WiFi mal sécurisées (ex. : depuis un café, un aéroport).

Cette prolifération des modes et des lieux de collecte, de traitement et de stockage des données, ainsi que la valeur croissante générée a incité la Commission de l'UE à actualiser ses réglementations pour mieux protéger la vie privée des citoyens et standardiser les lois de protection

Le Règlement Général sur la Protection des Données de l'UE (en anglais : GDPR ou General Data Protection Regulation), entrera en vigueur le 25 mai 2018 avec l'objectif de mieux protéger la façon dont les informations personnelles des citoyens européens sont collectées, traitées et stockées.

A qui le RGPD s'applique-t-il ?

Il s'applique à toutes les entreprises basées dans l'UE mais aussi à celles amenées à traiter les données de citoyens de l'UE. Au sein d'une entreprise, le RGPD doit être appliqué par les contrôleurs de données et par toutes les personnes traitant ces données. De plus, les entreprises doivent savoir parfaitement où et dans quelles conditions les données qu'elles collectent et stockent se trouvent physiquement, surtout si elles utilisent des solutions SaaS et des environnements cloud et hybrides.

Sous peine de se voir infliger de lourdes sanctions financières pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires annuel pour toute organisation déclarée non conforme, les entreprises doivent prendre les devants et déterminer quelles données elles ont en leur possession et comment s'y prendre pour se mettre en conformité.

Comment se mettre en conformité avec le RGPD ?

Les entreprises doivent comprendre quelles sont les nouvelles obligations qu'impose le RGPD et quel en sera l'impact sur les processus, les règles, la formation, les technologies utilisées et la sécurité des données qu'elles collectent et traitent. Les équipes informatiques et celles en charge de la conformité doivent considérer les étapes suivantes dans le cadre d'une démarche proactive de mise en conformité :

1 IDENTIFIER LES DONNÉES EN VOTRE POSSESSION :

Les entreprises doivent avoir une vision complète de toutes les données concernées en leur possession en vue d'appliquer les changements nécessaires pour se mettre en conformité. Toutefois, compte tenu de la complexité des environnements IT hybrides et de la prolifération des données dans toute l'organisation (ex. sur les appareils personnels), ce n'est pas chose aisée. Les entreprises doivent identifier :

a. ***Où*** se trouvent les données. Les entreprises doivent dresser le profil complet de toutes les données concernées qui sont en leur possession, qu'elles soient physiques ou numériques.

b. Qui a ***accès*** aux données. Les entreprises doivent s'assurer que les données à caractère personnel ne seront accessibles uniquement que les employés en ayant besoin pour mener à bien leur travail.

c. Comment les données sont ***traitées et transmises***. Au sein d'une organisation, les données sont transmises en interne mais peuvent aussi être envoyées en dehors du réseau, à des prestataires externes par exemple, et stockées sur plusieurs serveurs.

2 ACTUALISER LA FORMATION DES SALARIÉS :

Le RGPD exige des organisations qu'elles soient capables de fournir les preuves de leur conformité. Une formation peut permettre d'éviter des failles et de renforcer sa mise en conformité. Le règlement imposant aux entreprises de signaler une faille aux autorités compétentes sous 72 heures, chaque salarié doit pouvoir identifier les cas d'infraction au RGPD et en informer sa direction au plus vite. Il peut s'agir d'une compromission de données perpétrée de l'extérieur par un individu malveillant ou du fait qu'un salarié ait pu avoir accès à des données sans y être normalement autorisé.

3 EXAMINER VOTRE CHAÎNE LOGISTIQUE :

Qui, mis à part vos salariés, a accès à vos données ? Pensez aux fournisseurs cloud, aux agences de marketing et aux applications SaaS de CRM, RH et gestion des achats. Vous devez vérifier que tous ont bien mis en place les règles nécessaires et les mesures de sécurité qui s'imposent pour garantir votre conformité aux règles chaque fois qu'ils stockent ou traitent vos données.

4 CONTRÔLER ET SURVEILLER TOUS LES ACCÈS À VOS DONNÉES :

Les entreprises doivent s'assurer que les données personnelles ne seront jamais accessibles à ceux qui n'en ont pas besoin et, le cas échéant, établir ce qu'il est autorisé ou interdit de faire avec ces informations. Donnez aux utilisateurs uniquement l'accès dont ils ont besoin en appliquant le principe du "moindre privilège" et générez des rapports de suivi des activités de sessions.

Comment Bomgar peut aider votre entreprise à se mettre en conformité avec le RGPD

Bomgar propose des Solutions d'Accès Sécurisés permettant aux entreprises de contrôler, surveiller et administrer l'accès aux systèmes et aux données sensibles, sans que cela n'impacte la productivité ni ne perturbe le fonctionnement des opérations. Bomgar permet aux utilisateurs d'accéder aux systèmes rapidement et en toute sécurité, tout en protégeant les identifiants et les terminaux des menaces. Avec Bomgar, mettez en place une véritable stratégie de "security by design" (ou "sécurité dès la conception").

- **Appliquez le principe du moindre privilège :** n'accordez l'accès aux données qu'à ceux qui en ont besoin et quand ils en ont besoin, avec des contrôles d'accès granulaires pour éviter l'approche "tout ou rien"
- **Encadrez la prolifération des privilèges :** identifiez, sécurisez et centralisez vos comptes privilégiés (dont les identifiants dormants), éliminez les mauvaises habitudes des salariés qui partagent ou notent leurs mots de passe sur papier et appliquez vos politiques de sécurité
- **Conservez un historique des sessions :** enregistrez toutes les sessions d'accès et l'activité de chaque session. Vous saurez ainsi qui a accédé à quel système et pour y faire quoi, ce qui vous permettra de prendre les mesures adéquates si nécessaire
- **Supprimez tous les chemins d'accès point à point :** l'architecture sécurisée de Bomgar bloque tous les chemins d'accès point à point à vos systèmes, sans connexion descendante, éliminant ainsi la nécessité d'utiliser des VPN
- **Chiffrez les communications :** avec les solutions Bomgar, les données (en transit ou stockées) des sessions des comptes privilégiés sont chiffrées en TLS 1.2
- **Sécurisez et protégez tous les comptes privilégiés :** les identifiants privilégiés sont stockés, renouvelés automatiquement et gérés dans un coffre-fort de mots de passe pour comptes privilégiés. Les utilisateurs privilégiés bénéficient de niveaux d'autorisation adaptés à leurs besoins, ce qui permet de créer un protocole d'attribution des privilèges à la demande fiable et efficace
- **Eliminez toute gestion manuelle des mots de passe et des contrôles d'accès :** automatisez l'injection automatique d'identifiants et instaurez l'accès sécurisé aux systèmes en un clic pour les salariés et les prestataires privilégiés
- **Instaurez des politiques de sécurité des données garantissant la conformité avec le RGPD :** intégrez vos fournisseurs d'identité et vos règles de sécurité aux solutions Bomgar

Les solutions RGPD de Bomgar

Les Solutions d'Accès Sécurisés de Bomgar permettent aux professionnels de la sécurité informatique de contrôler et de gérer les accès aux systèmes sensibles par les utilisateurs privilégiés. Bomgar Remote Support et Bomgar Privileged Access s'intègrent avec Bomgar Vault. Cela permet de garantir une véritable stratégie de protection en défense et une productivité optimale.

REMOTE SUPPORT:
Simplifie le support, renforce la sécurité et optimise l'efficacité de votre support technique.

PRIVILEGED ACCESS:
Permet aux professionnels de la sécurité IT de contrôler et gérer les accès privilégiés aux systèmes critiques sans VPN.

PASSWORD VAULT:
Stocke et gère les identifiants partagés et les mots de passe pour les utilisateurs privilégiés.

Etre en conformité avec le RGPD

Bomgar vous aide à être en conformité avec plusieurs articles du RGPD et ainsi à réduire les risques liés aux accès à distance.

RÉSUMÉ DE L'ARTICLE	ÉLÉMENTS DE RÉPONSE BOMGAR
ARTICLE 5 – Principes relatifs au traitement des données à caractère personnel : les entreprises doivent mettre en place des mesures d'ordre technique et organisationnel appropriées pour garantir leur conformité et pouvoir en justifier, y compris des mesures de formation du personnel et de mesures de sécurité mises à jour régulièrement.	Les Solutions d'Accès Sécurisés Bomgar permettent aux entreprises d'avoir accès à distance et en toute sécurité aux terminaux, systèmes et utilisateurs. Avec des fonctions comme l'authentification sécurisée à deux facteurs, les permissions granulaires, les protocoles d'approbation, les enregistrements automatiques, le chiffrement et un grand choix d'options de déploiement, Bomgar aide les entreprises à se conformer aux standards de sécurité en vigueur. Bomgar permet un contrôle granulaire des accès et privilèges des utilisateurs. Tout le trafic transite par des ports standard. Les techniciens peuvent paramétrer des permissions de session granulaires et configurer des paramètres, comme des plages horaires et des zones d'accès spécifiques. Les accès peuvent aussi être approuvés au cas par cas. Les sessions se ferment automatiquement dès que le délai est écoulé. Les techniciens peuvent installer des Jump Clients (proxy Bomgar) pour les systèmes les plus fréquemment utilisés et utiliser des protocoles existants, dont RDP, Vpro, SSH Telnet, SUDO, etc. Tous les accès peuvent être enregistrés automatiquement pour analyses et audits ultérieurs, permettant à l'organisation de prouver sa conformité et de fournir les attestations nécessaires.

RÉSUMÉ DE L'ARTICLE	ÉLÉMENTS DE RÉPONSE BOMGAR
ARTICLE 7 – Conditions de consentement : chaque personne doit consentir à la collecte et au traitement de ses données à caractère personnel à des fins déterminées. La personne concernée a le droit de retirer son consentement à tout moment.	Dans le cas d'une prise en main à distance, le technicien peut configurer et personnaliser les champs d'information Bomgar requis pour le démarrage d'une session. L'utilisateur reçoit automatiquement une notification pour s'assurer de son consentement explicite avant de début de la session. Il peut à tout moment modifier ou annuler son consentement.
ARTICLE 15 - Droit d'accès par la personne concernée : la personne concernée est en droit de savoir si et où ses données personnelles sont traitées. Elle peut en faire la demande auprès du contrôleur des données à tout moment.	Les informations enregistrées par nos clients via les solutions Bomgar peuvent être extraites et récupérées si nécessaire. Les techniciens peuvent retrouver l'information correspondant à la demande d'une personne concernée en particulier.
ARTICLE 17 – Droit à l'oubli numérique et à l'effacement : le RGPD renforce les droits des personnes concernées. Celles-ci peuvent exiger d'avoir accès à leurs données personnelles telles que définies par le RGPD et détenues par une organisation ; elles peuvent également demander à faire valoir le droit à l'oubli, ce qui suppose que l'organisation doit avoir mis en place des processus pour effacer ces données.	Quiconque utilise Bomgar, que ce soit un technicien du support technique ou un client bénéficiaire du support, a le droit à l'oubli. Le technicien peut rechercher un utilisateur en particulier et le supprimer de la base ou l'anonymiser. Des règles de conservation personnalisables permettent à l'entreprise de décider de la durée de rétention des données et du type de données qu'elle souhaite conserver pour se mettre en conformité (plus de détails dans le Guide Admin de Bomgar).
ARTICLE 18 - Droit à la restriction du traitement : les individus sont en droit de restreindre le traitement de leurs données personnelles. La personne concernée doit donner son consentement préalable avant que les données ne puissent être traitées.	Bomgar permet aux techniciens de garantir que le consentement au traitement a bien été obtenu. L'utilisateur reçoit automatiquement une notification pour s'assurer de son consentement explicite avant de début de la session. Le consentement ou le refus est enregistré automatiquement dans les produits Bomgar.
ARTICLE 20 - Droit à la portabilité des données : les individus sont en droit de demander à recevoir les données personnelles les concernant détenues par une société dans un format exploitable et lisible. Ils sont autorisés à partager ces données avec une autre entreprise.	Bomgar permet au technicien de fournir un rapport regroupant les détails de la session relatifs à la personne concernée, sous format XML.
ARTICLE 25 – Protection des données dès la conception et par défaut : cet article établit que le responsable du contrôle des données doit mettre en œuvre des mesures d'ordre technique et organisationnel appropriées pour garantir que, par défaut, seules les données nécessaires dans le cadre d'une action spécifique ne seront traitées. Par ces mesures, les entreprises doivent s'assurer par défaut que les données personnelles ne seront pas accessibles à ceux qui n'en ont pas besoin.	Bomgar permet l'authentification sécurisée à deux facteurs via RADIUS, Smart Cards ou Bomgar Verify. Cela permet aux utilisateurs de s'authentifier via l'appareil de leur choix tel qu'un smartphone ou un PC portable. Il est possible d'intégrer à Bomgar des solutions de gestion des identités comme LDAP(s) ou Active Directory pour permettre le contrôle granulaire des règles de groupe. Bomgar permet un contrôle granulaire des accès et privilèges des utilisateurs. Tout le trafic transite par des ports standard. Les techniciens peuvent paramétrer des permissions de session granulaires et configurer des paramètres, comme des plages horaires et des zones d'accès spécifiques. Les accès peuvent être approuvés au cas par cas. Les sessions se ferment automatiquement dès que le délai est écoulé.

RÉSUMÉ DE L'ARTICLE	ÉLÉMENTS DE RÉPONSE BOMGAR
ARTICLE 32 – Sécurité du traitement : les entreprises doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir la sécurité des données : qui peut y accéder, quelle est la méthode de chiffrement etc.	Les techniciens peuvent créer des profils fournisseur et utilisateur avec des permissions spécifiques pour gérer efficacement les fournisseurs et les utilisateurs privilégiés. Si une intégration est faite avec l'annuaire d'entreprise, ce dernier applique les procédures en vigueur pour la création, la modification et la sauvegarde des mots de passe. La création de rapports à la demande permet au technicien de générer un rapport indiquant l'identité des personnes ayant eu accès aux données et aux systèmes. Tous les flux de données sont chiffrés et les données stockées sont disponibles quelle que soit la configuration afin de conserver des historiques et des enregistrements de session en toute sécurité. Des mises à jour et correctifs de sécurité sont proposés régulièrement.
ARTICLE 33 – Notification à l'autorité de contrôle d'une violation de données à caractère personnel : les entreprises s'engagent à notifier l'autorité de contrôle compétente dans les 72 heures au plus tard après avoir pris connaissance d'une violation et à décrire la nature de la violation de données y compris, si possible, les segments et la quantité approximative de données concernées par la violation.	L'activité de la session est enregistrée automatiquement et la solution permet de produire des rapports complets pour analyse. Bomgar peut aussi s'intégrer avec des outils SIEM pour l'analyse avancée des journaux d'activités. Il est possible de programmer des alertes en cas d'utilisation anormale ou d'activité suspecte. Des mesures préventives peuvent aider à réduire le risque de compromission. Des sessions peuvent être autorisées au cas par cas et des protocoles peuvent être configurés via des outils intégrés de gestion du changement. Il est possible de restreindre l'accès de façon granulaire. La rotation des identifiants dès la fin de la session garantit la disponibilité optimale des identifiants.

Ce protocole est applicable avec la version 18.1 de Bomgar Remote Support, Privileged Access et Vault. Il est possible que les versions précédentes de ces solutions ne permettent pas de répondre aux exigences détaillées ci-dessus.

(1) http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
(2) http://www.bbc.co.uk/news/business-39947942
(3) https://www.bomgar.com/resources/whitepapers/secure-access-threat-report

A PROPOS DE BOMGAR

Bomgar est le leader des solutions d'accès sécurisés pour les entreprises. Les solutions Bomgar pour le support et la prise en main à distance, et pour la gestion des accès privilégiés et des identifiants aident les professionnels du support et de la sécurité informatiques à améliorer leur productivité et la sécurité de leurs systèmes en proposant des connexions fiables et contrôlées à tout type de système ou périphérique, partout dans le monde. Plus de 12 000 entreprises dans 80 pays utilisent Bomgar pour fournir des services d'assistance de qualité et réduire les risques de menaces sur les données et les systèmes critiques. Bomgar est une entreprise privée et possède des bureaux à Atlanta, Jackson, Washington D.C., Francfort, Londres, Paris et Singapour. Connectez-vous à Bomgar : visitez www.bomgar.fr.

CONTACT | INFO@BOMGAR.COM | +33 (0)1 44 75 75 80 | BOMGAR.COM/FR

©2017 BOMGAR CORPORATION. TOUS DROITS RÉSERVÉS DANS LE MONDE. BOMGAR ET LE LOGO BOMGAR SONT DES MARQUES DÉPOSÉES DE BOMGAR CORPORATION. LES AUTRES MARQUES MENTIONNÉES SONT LA PROPRIÉTÉ DE LEURS PROPRIÉTAIRES RESPECTIFS.