POLITIQUE GENERALE DE PROTECTION DES DONNEES PERSONNELLES

Titre	Politique générale
Sous-titre	Politique générale de protection des données personnelles
Catégorie	Procédure interne
Version	1.2
Diffusion	Interne
Date de création	09 /2021
Responsable du document(s)	
Contributeur(s)	
Approbateur(s)	
Niveau de confidentialité	Interne

Peers Group

1. Introduction

La Politique de protection des données personnelles décrit les dispositions prises par PEERSGROUP pour traiter les données à caractère personnel des clients, des fournisseurs, des collaborateurs et des candidats dans le cadre des activités de PEERSGROUP.

PEERSGROUP s'est engagé dans un processus d'amélioration continue, cette politique est amenée à évoluer. PEERSGROUP assurera une communication permanente par la mise à jour de la présente politique de sécurité vers les clients, les fournisseurs et les utilisateurs afin qu'ils restent informés des évolutions de la politique de sécurité.

2. Objectif de cette politique

- L'objectif de cette Politique est de décrire quelles données personnelles nous collectons, dans quel but nous les recueillons et les utilisons, et avec qui nous les partageons ;
- Définir vos droits et choix relatifs aux données personnelles que nous collectons et traitons, et expliquer comment nous protégeons votre vie privée ;

Nous espérons que cette Politique vous aidera à comprendre nos engagements pour protéger votre confidentialité et votre vie privée.

3. Périmètre

Cette politique des mesures de protection concerne PEERSGROUP.

4. Besoin de sécurité

PEERSGROUP s'est engagé dans une démarche d'amélioration continue de la sécurité du système d'information, notamment les données personnelles. Nous réévaluons l'analyse de nos risques en permanence et à chaque nouvelle activité pour assurer un niveau cohérent de sécurité dans le traitement des projets de nos clients et sous-traitants.

5. Aspect légal

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après dénommé « **RGPD** ») venant modifier la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après dénommée « loi informatique et Libertés) introduit de nouvelles règles applicables.

6. Définitions

« **Utilisateur** » est la personne autorisée à accéder aux ressources informatiques et à les utiliser. Il s'agit notamment des employés de l'Entreprise, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels.

« **Le Système d'information** » est un ensemble organisé de Ressources qui permet de collecter, stocker, traiter et distribuer de l'information via le Réseau.

« **Les Données de l'entreprise** » englobent les informations techniques (méthodes, études spécifiques, savoir-faire), les informations commerciales (fichiers clients, fichiers fournisseurs, plans marketing, canaux et méthodes de distribution, résultats d'enquêtes marketing), les informations économiques et financières (contenu des offres et propositions commerciales, prix d'achat et de vente, montage

juridique et financier, conditions de contrat, assurances) et les informations stratégiques et organisationnelles (projets de rapprochements, projets de recrutement, synthèses résultants de la veille stratégique et technologique).

« **Les Données personnelles** » constitue toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un ou plusieurs éléments qui lui sont propres tels un nom, un numéro d'identification, des données de géolocalisation, un identifiant en ligne ou à un ou plusieurs facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne physique. Une adresse IP, des informations relatives à la vie professionnelle sont des exemples de données personnelles.

« **Le Traitement** » est défini comme toute opération, ou ensemble d'opérations, portant sur des données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction ...).

7. Procédure d'évolution et mise à jour

Toutes les évolutions de cette politique sont soumises à l'approbation de la direction de l'entreprise et sur les conseils de notre DPO. Elles peuvent porter sur de nouvelles conditions liées au processus d'exploitation et des évolutions faisant suite au plan d'amélioration continue. En cas de modification de cette Politique, nous vous en informerons par le biais de notifications adaptées, notamment e-mail.

8. Responsabilité

La responsabilité de l'application du RGPD dans l'entreprise et des interactions avec les clients et sous-traitants est directement placée sous la direction de PEERSGROUP.

8.1. Nous contacter

Si vous avez des questions sur cette Politique, vous pouvez contacter notre responsable à la protection des données en utilisant les moyens mis à votre disposition ci-dessous :

Contacter le DPO par courriel : rgpd@peersgroup.fr

9. Sensibilisation et communication

PEERSGROUP veille à la sensibilisation des utilisateurs traitant des données personnelles. La conformité de PEERSGROUP fait l'objet d'une communication et d'une présentation périodique auprès des services et des utilisateurs de PEERSGROUP.

10. Application du Privacy by default et Design

PEERSGROUP en tant que responsable de traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut ou lors de la mise en œuvre de nouvelles activités ou de nouveaux développements dans le cadre de la fourniture du logiciel de PEERSGROUP, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.

Application du Privacy By Default et Design :

- Volume de données à caractère personnel collectées ou traitées
- Nature des données (sensibles, etc.) et catégories de personnes concernées
- Etendue de leur traitement
- Durée de conservation et accessibilité
- Finalité et licéité des traitements

Destinataires des données

11. Politique de collecte des données personnelles

11.1. Type de données personnelles collectées

Les données collectées sont les Données de l'entreprise et les Données personnelles relatives aux clients, aux fournisseurs, aux collaborateurs et aux candidats.

11.2. Utilisation des données personnelles

Vos données sont à destination exclusive des utilisateurs habilités au sein de la société PEERSGROUP. Les traitements réalisés par des sous-traitants sont répertoriés dans nos registres de Traitements.

11.3. Conservation et suppression des données

La conservation et la suppression des données est formalisées dans nos registres de traitements et encadrée par des procédures.

11.4. Transfert dans d'autres pays

Aucune donnée personnelle n'est transférée en dehors de l'Union européenne.

11.5. Respect du droit des personnes

Conformément à la loi Informatique et Libertés n° 78-17 du 6 janvier 1978 et du règlement européen (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 sur la protection de la donnée personnelle et de manière générale à la réglementation française et européenne relative à la
Conformément à la loi Informatique et Libertés n° 78-17 du 6 janvier 1978 telle que modifiée et du règlement européen (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 sur la protection de la donnée personnelle, les personnes concernées peuvent exercer leur droit d'accès aux données à caractère personnel les concernant et, le cas échéant, leur droit de rectification et de suppression et d'effacement et notamment si les données sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Les personnes concernées peuvent également s'opposer, pour des motifs tenant à leur situation personnelle, au traitement de leurs données à caractère personnel ou exercer leur droit à la portabilité de leurs données, dans les conditions prévues par la réglementation.

Ces droits peuvent être exercés par courrier adressé à PEERSGROUP :

Contacter le DPO par courriel : rgpd@peersgroup.fr

12. Traitements des données

12.1. Sous-traitants

PEERSGROUP est soucieux de confier le traitement des données de PEERSGROUP et des clients de PEERSGROUP à des sous-traitants qui présentent des garanties suffisantes en matière de protection des données personnelles et encadrés par des contrats de prestation.

12.2. Sécurité des traitements Analyse d'impact

Dans les cas prévus par la réglementation et conformément aux délibérations de la CNIL, lorsque les traitements font peser des risques élevés pour les droits des personnes, PEERSGROUP procèdera à des analyses d'impact. Notre méthodologie se base sur l'outil PIA de la CNIL.

13. Gestion des incidents

Pour faire face à un incident de sécurité et prendre les décisions pertinentes pour gérer l'incident, PEERSGROUP a mis en place une procédure de gestion des violations des données personnelles.

14. Amélioration continue

PEERSGROUP s'est engagée dans un processus d'amélioration continue sur la pertinence, l'adéquation et l'efficacité de la conformité du RGPD.

L'objectif du processus d'amélioration continue est d'évaluer périodiquement par un programme d'audit interne les écarts avec le règlement et de faire évoluer notre conformité et notre sensibilisation au règlement et ses évolutions. Cette démarche est placée sous la responsabilité de la direction.

PEERSGROUP prend en compte les résultats des analyses et des évaluations, ainsi que les éléments de sortie de la revue de direction pour déterminer s'il existe des besoins ou des opportunités à considérer dans le cadre de l'amélioration continue.

15. Sécurité des données personnelles

Nous nous engageons à protéger les données personnelles de nos clients et utilisateurs. Nous mettons en œuvre des mesures techniques et organisationnelles appropriées afin de protéger la sécurité de vos données personnelles.

Nous avons mis en place diverses politiques, y compris des politiques de pseudonyme, de chiffrement, d'accès et de conservation visant à empêcher tout accès non autorisé et toute conservation inutile des données personnelles dans nos systèmes.

15.1. Contexte de la politique de mesures de protection des données

Dans le cadre de [article 32] du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection à caractère personnel, PEERSGROUP a renforcé les mesures de protection selon les risques inhérents à PEERSGROUP pour définir les mesures à mettre en œuvre et approprié à notre environnement.

15.2. Relation avec les fournisseurs impliqués dans le système d'information

PEERSGROUP peut avoir recours à des sous-traitants de données personnelles pour assurer la délivrance des activités de PEERSGROUP. Les sous-traitants sont évalués sur leur mise en conformité et font l'objet d'une évaluation annuelle dans le cadre de notre amélioration continue.

15.3. Protection physique

15.3.1. Accès aux données sur site

L'accès aux locaux se fait par empreintes digitales 24 heures sur 24. Une journalisation assure la traçabilité des accès.
Un agent de sécurité surveille les locaux 24 heures sur 24.

15.3.2. Accès aux Datacenters

PEERSGROUP a fait le choix de Datacenter présentant des sécurités suffisantes pour l'hébergement des données. Nos données sont hébergées chez Microsoft :

15.4. Accès au système d'information et habilitations

L'accès au système d'information est un élément essentiel de notre politique de sécurité de l'information. PEERSGROUP protège efficacement la confidentialité, l'intégrité et la disponibilité des données.

15.4.1. Gestion des accès utilisateurs

Chaque accès au système d'information est subordonné par un compte utilisateur/Mot de passe unique à chaque utilisateur. Les mots de passe sont soumis à des politiques de complexité et de changement forcé périodiquement (annuellement). Le système d'information est composé de la messagerie Microsoft Office 365, l'accès aux fichiers bureautiques hébergé sous environnement Microsoft et des applications hébergées par nos prestataires.

15.4.2. Création, suppression et ajustement

PEERSGROUP a une procédure de contrôle des créations et suppressions de comptes validée par le service des ressources humaines. Cette procédure permet de contrôler que seuls des utilisateurs validés puissent accéder au système d'information et selon des habilitations précises. Le référentiel nous permet de réviser régulièrement lors des audits internes que les utilisateurs sont bien accrédités à se connecter au système d'information.

15.5. Traçabilité

La journalisation est l'outil le plus approprié pour PEERSGROUP pour suivre et surveiller l'activité sur le système d'information. Nous surveillons en temps réel les accès et les tentatives d'accès aux fichiers et répertoires ainsi que sur nos applications métiers sensibles stockées sur nos serveurs. La traçabilité nous fournit des rapports complets et précis sur les accès inappropriés, l'altération ou la destruction de fichiers, de dossiers ou de partages de fichiers.

15.6. Accès réseau

Les accès réseau se font de deux façons, le réseau Wifi et réseau câblé.

15.6.1. Réseau Wifi

Privé
les utilisateurs se connectent via une borne Wifi sécurisée par une clé de sécurité.

15.7. Réseau câblé

L'accès au réseau câblé est uniquement disponible aux équipements d'impression de PEERSGROUP. La charte informatique interdit toute connexion d'un autre équipement que ceux de PEERSGROUP.
Les accès réseau se font par réseau câblé. L'accès au réseau câblé est uniquement disponible aux équipements d'impression de PEERSGROUP.

15.1. Internet

Les connexions via le réseau Internet font l'objet d'équipement de filtrage afin d'assurer un contrôle sur les flux échangés et prévenir les cyberattaques.

15.2. Sécurité des équipements informatiques

Les équipements destinés aux utilisateurs, concerne : les ordinateurs fixes et portables, les téléphones mobiles.

- Restriction des droits d'administration des équipements
- Protection antivirale centralisée
- Planification des mises à jour, notamment de sécurité centralisée

- Chiffrement des disques durs dès la mise à disposition des équipements

15.3. Serveur de stockage

PEERSGROUP bénéficie des mesures de sécurité suivantes :

- Restriction des droits utilisateurs
- Habilitation sur les espaces de stockages
- Protection antivirale
- Planification des mises à jour, notamment de sécurité
- Surveillance en temps réel via la supervision
- Garantie constructeur

15.4. Authentification des accès distants

L'accès distant fait partie intégrante des activités de PEERSGROUP, un utilisateur peut se connecter à distance dans le cadre de ses missions. L'accréditation est autorisée par les responsables et communiquée dans la fiche d'accréditation d'entrée. Les accès sont sécurisés par un accès VPN SSL unique à chaque utilisateur. Les accès distants sont uniquement accessibles aux équipements de PEERSGROUP.

Chiffrement

Pour garantir la confidentialité des données personnelles et plus largement des bases de données des clients de PEERSGROUP, toutes les bases de données sont chiffrées avec un mécanisme 256 Bits, rendant l'accès aux données impossibles en cas de vol ou d'accès malveillant.

Commenté [DMS1]: En attente d'une réponse pour demain 15/09 (microsoft)

15.5. Manipulation des supports

Pour empêcher la divulgation et la fuite d'information lors du retrait d'équipement informatique, PEERSGROUP procède à la suppression des données des équipements avant transfert physique des supports.

15.6. Transfert de l'information

PEERSGROUP a communiqué dans le cadre de la charte informatique des procédures strictes en matière de procédure de transfert de l'information des données personnelles. Celle-ci ne doit plus être transmise par la messagerie électronique.

15.7. Plan de reprise d'activité

Le plan de reprise d'activité est en cours de formalisation dans la procédure et le recensement de nos processus de sauvegarde. Le plan de reprise d'activité sera testé et fait partie intégrante de notre processus d'amélioration continue.

16. Revue de la sécurité de l'information

PEERSGROUP a intégré la revue des mesures de protection dans le cadre de l'amélioration continue et des audits internes. PEERSGROUP évalue ses risques périodiquement en fonction des nouvelles activités et menaces. Les mesures de protection sont réadaptées.