Politique de protection des données personnelles
Applicable à l'ensemble des filiales de blis

1. Objectif

blisgroup s'engage, dans le cadre de ses activités et conformément à la législation en vigueur en France et en Europe, à assurer la protection, la confidentialité et la sécurité des données à caractère personnel des utilisateurs de ses services, ainsi qu'à respecter leur vie privée.
La présente Politique informe sur la façon dont blisgroup, ses sous-traitants et ses éventuels partenaires traitent les données personnelles.

L'entreprise restreint également l'accès aux données confidentielles et sensibles pour éviter qu'elles ne soient perdues ou compromises, de façon à ne pas nuire à nos clients, à ne pas encourir de sanctions pour non-conformité et à ne pas nuire à notre réputation. Parallèlement, nous devons faire en sorte que les utilisateurs puissent accéder aux données qui leur sont nécessaires pour travailler efficacement.

Il n'est pas attendu de cette politique qu'elle élimine tous les vols de données. Son principal objectif est plutôt de sensibiliser les utilisateurs et d'éviter les scénarios de perte accidentelle, c'est pourquoi elle décrit les exigences de prévention des fuites de données.

2. Champ d'application

2.1 Dans le champ d'application

Cette politique de sécurité des données s'applique à toutes les données clients, données personnelles ou autres données de l'entreprise définies comme sensibles. Elle s'applique donc à tous les serveurs, bases de données et systèmes informatiques qui traitent ces données, y compris tout appareil régulièrement utilisé pour le courrier électronique, l'accès au Web ou d'autres tâches professionnelles. Tout utilisateur qui interagit avec les services informatiques de l'entreprise est également soumis à cette politique.

2.2 Hors du champ d'application

Les informations classées comme publiques ne sont pas soumises à cette politique. D'autres données peuvent être exclues de la politique par la direction de l'entreprise, en fonction d'impératifs spécifiques, par exemple le fait que la protection des données est trop coûteuse ou trop complexe.

3. Politique

3.1 Principe général

Pourquoi blisgroup traite ces données ?
blisgroup traite les données personnelles dans le cadre de l'exécution d'un contrat de transport. A cet effet, les finalités sont les suivantes :

- Gérer l'identité du client ou de l'utilisateur et l'authentifier
- Gérer la commande ou la demande de devis
- Gérer les contacts à l'enlèvement et à la livraison
- Facturer et encaisser les paiements
- Assurer le service avant-vente et après-vente
- Assurer le suivi du transport
- Assurer la communication de l'état d'avancement du transport
- Recouvrer les impayés
- Gérer les contentieux

Siège social : 41 Rue de la Burelle – 45800 SAINT JEAN DE BRAYE - Tél. 02 38 83 83 00 – Fax 02 38 86 56 57
Direction Commerciale : 32 Avenue de l'Océanie – Zone de Courtaboeuf - Bâtiment A - Quai 15 - 91140 VILLEJUST
RCS Orléans - N° SIRET 511 564 916 00019 - SARL au capital de 10 000 € - APE 7022 Z -
N° de TVA intracommunautaire FR 45 511 564 911

Les données sont conservées pour la durée nécessaire à l'accomplissement des finalités mentionnées ci-dessus.

blisgroup peut également réaliser des traitements de données pour d'autres finalités que la stricte exécution du contrat transport. Les finalités poursuivies sont les suivantes :

- Organiser des opérations d'information et de marketing direct.
- Sonder les clients ou les utilisateurs
- Améliorer les offres et la relation client
- Traitement des données à des fins statistiques. blisgroup ne commercialise pas les statistiques obtenues

Les données sont conservées pour la durée nécessaire à l'accomplissement des finalités mentionnées ci-dessus.

blisgroup traite également les données pour répondre à ses obligations légales ou réglementaires. Les finalités poursuivies sont les suivantes :

- Conserver les données requises pour être mesure de répondre aux obligations légales
- Gérer les demandes de communication de données des autorités habilitées

Les données peuvent être conservées le temps nécessaire pour permettre à blisgroup de répondre à ses obligations légales.

Quelles sont les données traitées ?

blisgroup traite les catégories de données suivantes :

- Données d'identification : Nom, prénom, raison sociale…
- Données de contact : adresse postale, email, numéro de téléphone…

Quels sont les destinataires des données ?
Les données collectées sont destinées aux services internes de blisgroup et à ses sous-traitants.

Les données sont-elles traitées hors UE ?
Dans le cas d'un transport exceptionnel, les données collectées sont susceptibles d'être traitées hors de l'Union Européenne. Dans ce cas, blisgroup prend les dispositions nécessaires avec ses sous-traitants et partenaires pour garantir un niveau de protection de vos données adéquates et ce en toute conformité avec la réglementation applicable.

Quels sont vos droits ?
Vous disposez d'un droit d'accès, de rectification et de suppression des données qui vous concernent. Vous pouvez demander la portabilité de ces dernières. Vous avez également le droit de vous opposer aux traitements réalisés ou d'en demander la limitation.

Vous pouvez émettre des directives sur la conservation, la suppression ou la communication de vos données personnelles après votre décès.

Règle spécifique au démarchage téléphonique : tout consommateur peut s'inscrire gratuitement sur une liste d'opposition dénommée « Bloctel » afin de ne plus être démarché téléphoniquement par un professionnel avec lequel il n'a pas de relation contractuelle en cours. Le consommateur peut s'inscrire sur le site www.bloctel.gouv.fr ou par courrier adressé à : Société Opposetel, Service Bloctel, 6, rue Nicolas Siret – 10 000 Troyes
Pour mettre à jour les données personnelles que nous traitons vous concernant, veuillez nous contacter sur serviceclient@blisgroup.com ou directement sur la page de contact de notre site blisgroupgroup.com.

Comment exercer vos droits ?
Vous pouvez exercer vos droits à tout moment, ainsi que contacter le Délégué à la Protection des Données personnelles, sur l'adresse e-mail serviceclient@blisgroupgroup.com ou directement sur la page de contact de notre site blisgroup.com. Toute demande d'exercice de vos droits doit être accompagnée de la photocopie d'un justificatif d'identité (carte nationale d'identité délivrée par l'Etat français ou carte d'identité de l'union Européenne ou passeport, carte de résident délivrée par l'Etat français, carte de séjour délivrée par l'Etat français ou livret de circulation délivré par l'Etat français). Une réponse vous sera adressée dans un délai d'un mois à compter de la réception de votre demande.
Possibilité de saisir la CNIL
Si vos échanges avec blisgroup n'ont pas été satisfaisants, vous avez la possibilité d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL), autorité de contrôle en charge du respect des obligations en matière de données à caractère personnel en France.
Comment les données sont-elles sécurisées ?

blisgroup s'assure que les données sont traitées en toute sécurité et confidentialité, y compris lorsque certaines opérations sont réalisées par des sous-traitants. A cet effet les mesures techniques et organisationnelles appropriées pour éviter la perte, la mauvaise utilisation, l'altération et la suppression des données personnelles vous concernant sont mises en place. Ces mesures sont adaptées selon le niveau de sensibilité des données traitées et selon le niveau de risque que présente le traitement ou sa mise en œuvre.

L'entreprise fournira à tous ses clients, employés et à ses sous-traitants l'accès aux informations dont ils ont besoin pour faire leur travail aussi efficacement que possible.

3.2 Organisation

a) Chaque utilisateur sera identifié par un ID utilisateur unique, afin que tous puissent être tenus pour responsables de leurs actions.

b) L'utilisation des identités partagées n'est autorisée que là où elles sont appropriées, par exemple pour les comptes de formation ou les comptes de service.

c) Chaque utilisateur doit lire la présente politique de sécurité des données, ainsi que les directives de connexion et de déconnexion, et signer une déclaration stipulant qu'ils comprennent les conditions d'accès.

d) Les enregistrements des accès des utilisateurs peuvent être utilisés comme éléments probants dans le cadre d'une enquête sur incident de sécurité.

e) Les accès doivent être accordés selon le principe du moindre privilège, ce qui signifie que chaque programme et chaque utilisateur obtiendra seulement les privilèges qui lui sont nécessaires pour effectuer son travail.

3.3 Autorisation de contrôle d'accès

L'accès aux ressources et aux services informatiques de l'entreprise sera accordé par le biais d'un compte d'utilisateur unique et d'un mot de passe complexe.

3.4 Accès aux réseaux

Un accès aux réseaux doit être accordé à tous les employés et sous-traitants, selon les procédures de contrôle d'accès de l'entreprise et le principe du moindre privilège.

3.5 Responsabilités des utilisateurs

a) Tous les utilisateurs doivent verrouiller leur écran chaque fois qu'ils quittent leur bureau, pour réduire le risque d'accès non autorisé.

b) Tous les utilisateurs doivent veiller à ne laisser aucune information sensible ou confidentielle autour de leur poste de travail.

c) Tous les utilisateurs doivent tenir leurs mots de passe confidentiels et ne pas les partager.

3.6 Accès aux applications et aux informations

a) Le système d'information est accessible via un login/Mot de passe propre à chaque utilisateur sur une plateforme internet. La connexion est conditionnée par un profil utilisateur. Celui-ci permet l'utilisation d'un menu limité à ses prérogatives.

b) Tous les employés et sous-traitants de l'entreprise doivent bénéficier d'un accès aux données et aux applications nécessaires à leur fonction professionnelle.

c) Tous les employés et sous-traitants ne doivent accéder aux données et systèmes sensibles qu'en cas de nécessité professionnelle et avec l'accord de la direction.

d) Les systèmes sensibles doivent être physiquement ou logiquement isolés afin d'en restreindre l'accès au personnel autorisé uniquement.

3.7 Accès aux informations confidentielles et restreintes

a) L'accès aux données classées comme « confidentielles » ou « restreintes » doit être limité aux personnes autorisées dont les responsabilités professionnelles l'exigent, tel que déterminé par la direction.

b) Le service de sécurité informatique est responsable d'instaurer les restrictions d'accès.

4. Directives techniques

Les méthodes de contrôle d'accès à utiliser incluent :

- Modèle d'accès basé sur les rôles
- Droits d'accès aux serveurs
- Séparation des réseaux

Le contrôle d'accès s'applique à tous les réseaux, serveurs, postes de travail, ordinateurs portables, appareils mobiles, applications Web, sites Web, stockages Cloud et services.

5. Responsabilités

- **L'administrateur de la sécurité des informations** est un employé chargé par les responsables informatiques d'assurer un soutien administratif pour l'implémentation, la supervision et la coordination des procédures et systèmes de sécurité, conformément aux ressources informatiques spécifiques.
- **Les utilisateurs** comprennent tous ceux qui ont accès aux ressources informatiques, par exemple les employés, les entités de confiance, les sous-traitants, les consultants, les employés à l'essai, les employés temporaires et les bénévoles.
- **L'équipe d'intervention en cas d'incident** est dirigée par le responsable informatique.

6. Application

Tout utilisateur qui enfreint cette politique est passible de sanctions disciplinaires, pouvant aller jusqu'au licenciement. Tout partenaire ou sous-traitant tiers surpris en infraction peut voir sa connexion au réseau suspendue.

Modification de la Politique de protection des données
La présente Politique de protection des données personnelles peut être amenée à évoluer.
Dernière mise à jour le 08/04/2019

Jean-Marc BREHERET
Gérant – Direction Générale