

Protection des données personnelles & Réglementation européenne

Dolist s'engage pour le respect des données et des internautes



Pensez à la planète !
Si vous souhaitez imprimer ce document, faites-le en noir & blanc ;)

29/06/2023

Introduction au RGPD

Le Règlement Général sur la Protection des Données (RGPD) correspond dans les faits à une officialisation d'une approche marketing déontologique et respectueuse des individus. Loin d'être un obstacle, nous y voyons une opportunité de recréer la confiance entre les marques et leurs publics. Une nécessité pour une performance durable des actions marketing et une conviction que nous avons pu vérifier depuis longtemps.

A l'image de nos préconisations et des obligations imposées par le RGPD, Dolist s'implique, en tant que responsable de traitement mais également en tant que sous-traitant, à sécuriser les traitements des données personnelles que nous réalisons pour le compte de nos clients.

Suite à l'entrée en application du RGPD en mai 2018, Dolist a entrepris une démarche de mise en conformité en matière de protection de données personnelles qui complète, dans les faits, les engagements qu'elle tient depuis de nombreuses années déjà.

Point sur la vision Dolist, nos engagements en matière de protection des données personnelles et d'accompagnement de nos clients.



En 2015, Jean-Paul Lieux, directeur associé de Dolist, affirmait déjà :

« Dolist est une aventure passionnante car elle combine des enjeux technologiques et humains. Nous sommes au cœur d'une évolution continue qui réinvente la relation entre les marques et le consommateur. Au-delà des challenges technologiques, nous avons donné à Dolist la mission d'accompagner ses clients pour optimiser l'efficacité de leurs programmes relationnels digitaux. Basée sur la pertinence de la data et sur une automatisation grandissante, cette relation doit aussi s'appuyer sur la confiance et le respect du consommateur. »

Sommaire

Introduction au RGPD	2
Marketing Digital, confiance & pertinence : le trio gagnant	4
RGPD : Cadre général & mise en application chez Dolist	5
Sécurité & aspects techniques	6
Mise en conformité RGPD & Accompagnement de nos clients	8
Protection des droits & information des personnes (en tant que responsable de traitement)	9
A propos de Dolist	10
Contactez-nous	10

Marketing Digital, confiance & pertinence : le trio gagnant

L'arrivée de la réglementation européenne a été, pour Dolist, un continuum logique de l'évolution des métiers du marketing, de la surexploitation des données personnelles et de la montée des craintes des consommateurs. En 2013 déjà, Dolist s'interrogeait dans un livre blanc sur « Comment le respect des règles déontologiques et législatives peut améliorer les performances de vos campagnes de Marketing Digital ? » et prenait clairement position :

« Non, l'e-marketing n'est pas synonyme de pillage systématique des données personnelles. Oui, il est possible de respecter le cadre législatif et les règles de déontologie en la matière pour améliorer l'efficacité des campagnes marketing. La performance durable du marketing est à la croisée des chemins, entre confiance et respect de la légalité. »

Un nécessaire retour à la confiance

Si longtemps les consommateurs ont accepté de fournir des données à caractère personnel via les sites web, bien souvent avec un défaut d'information quant aux utilisations qui en seraient faites, les nombreuses amendes prononcées depuis 2018 par la CNIL contre des entreprises emblématiques comme Google, Youtube, Facebook, Amazon, Microsoft, Carrefour, Totalenergie, EDF, Accor, Free et Free Mobile ont généré des comportements de méfiance de bon nombre d'internautes voire, pour certains, le refus catégorique de fournir leurs données personnelles.

Le retour à la confiance passe aujourd'hui inévitablement par la transparence sur les raisons et la finalité de l'utilisation des données personnelles et la réelle prise au sérieux des enjeux de la sécurisation de celles-ci.

Une attitude marketing responsable

Fini le temps où les marques pouvaient, en toute impunité, envahir les messageries des consommateurs par des e-mails non sollicités. Aujourd'hui, la majorité d'entre nous a atteint une maturité digitale qui exige de la part des marques une attitude responsable dans leurs opérations marketing.

C'est d'ailleurs sur ces comportements éthiques envers la collecte et le traitement des données personnelles des consommateurs qu'on observe aujourd'hui une différence entre les concurrents. Les marques respectueuses des données personnelles sont davantage plébiscitées par les consommateurs et donc clairement gagnantes.

Reconnaissance et personnalisation des opérations

Ainsi, les consommateurs attendent des offres et des envois adaptés à leurs profils. Là où certains peuvent se contenter de recevoir de façon irrégulière les informations d'une marque, le futur client attend d'être bien identifié et traité avec égard par des envois réguliers d'informations, d'offres ou de promotions personnalisés. Une telle stratégie nécessite toutefois de connaître parfaitement bien

ses clients et donc de collecter auprès d'eux et en toute transparence les bonnes données, sans avoir une attitude invasive contre-productive.

Au-delà des aspects législatifs, une stratégie marketing efficiente développe une attitude marketing responsable et durable. Il ne faut jamais oublier que derrière les données se trouvent des individus. Le marketing digital impose plus que jamais aux marques de remettre le client au centre de leurs préoccupations sans le réduire à de simples statistiques ou bases de données.

RGPD : Cadre général & mise en application chez Dolist

- **Désignation dès 2018 d'un Délégué à la Protection des Données (ou « Data Privacy Officer »/ DPO)**, référent et pilote de la conformité RGPD au sein de l'entreprise, en charge de la protection des données, de la sensibilisation des collaborateurs et du suivi de l'évolution du traitement des données.
Le DPO de Dolist est la société DIGITEMIS, qui peut être contactée à l'adresse dpo@dolist.com.
- **Mise en place d'un registre des traitements des données personnelles**, recensant l'ensemble des activités conduisant l'entreprise à traiter des données personnelles, décrivant entre autres la finalité de chaque traitement, les catégories de données traitées, les destinataires, la durée de conservation, les transferts de données hors UE et les mesures de sécurité mises en place.
- **Sensibilisation du personnel** aux enjeux de confidentialité et de sécurité des données, mise en place de sessions de formation ainsi que d'accords de confidentialité et de sécurité.
- **Limitation des manipulations de données de nos clients** aux seules prestations qui nous sont confiées en tant que sous-traitant et aux seules personnes habilitées pour les réaliser.
- **Vérification que nos partenaires et sous-traitants** ayant éventuellement accès aux données ou étant en lien avec la gestion des données **respectent les obligations** de sécurité et de protection des données.
- **Adhésion aux codes de bonnes conduites professionnelles** du secteur : Membre de Signal Spam, Dolist adhère à sa charte déontologique depuis 2004. Depuis 2009, nous sommes également membre du MAAWG (Messaging Malware Mobile), groupe de travail international visant à lutter contre tous les types d'abus sur Internet et améliorer la protection des utilisateurs finaux. Une collaboration qui nous permet de faire constamment évoluer nos technologies, nos process de sécurité et d'accompagner nos clients vers des pratiques plus déontologiques et efficaces. En 2022, Dolist signe la charte de l'Institut du Numérique Responsable (INR) s'engageant ainsi à s'évaluer et à mettre en œuvre une série d'actions dans une logique d'amélioration continue pour contribuer, à son échelle, à un numérique plus responsable et à la diffusion de ses bonnes pratiques.

Sécurité & aspects techniques

- **Réalisation d'un audit de sécurité.** Afin de certifier l'ensemble de nos prestations et services, nous faisons appel au cabinet DIGITEMIS (<https://www.digitemis.com/> - Qualification PASSI par l'ANSSI) qui a conduit un audit complet allant des pratiques et méthodes de traitement aux infrastructures techniques.
- Effectuer régulièrement des **tests techniques d'intrusion** et tenir un registre des incidents de sécurité. L'objectif est de valider l'étanchéité totale de notre organisation en matière de données utilisateurs. Ces derniers sont réalisés régulièrement depuis 2015.
- Mise en place en 2016 d'une **Politique Générale de Sécurité de l'Information** (PGSI) au sein de DOLIST afin d'organiser et encadrer les aspects de sécurité.
- **Authentification client, sécurisation et traçabilité des accès** aux technologies Dolist (mots de passe cryptés, des utilisateurs, HTTPS...)
- **Transmission des données clients** via des canaux sécurisés HTTPS/FTPS/SFTP.
- **Données clients disponibles et conservées** pendant toute la durée de la relation contractuelle. Le client est responsable de récupérer ces données avant la suppression du compte au terme du contrat. Une fois le compte supprimé, les données sont archivées pendant 3 mois avant suppression définitive (sous réserve des instructions du client).
- **Durée de conservation** des données utilisateurs :
 - Technologies V8/CAMPAIGN : données personnelles conservées tant que le compte client existe et données comportementales conservées 2 ans. Au-delà, elles sont agrégées et anonymisées pour maintenir une représentation des statistiques. Ces dernières sont sauvegardées dans un fichier au format ZIP disponible pour le client pendant 30 jours sur son espace FTP sécurisé.
 - Technologies EMT : données personnelles conservées tant que le compte client existe. Les données comportementales et logs sont conservés 180 jours par défaut (au-delà les données sont supprimées et agrégées pour les statistiques). Le contenu des messages est, quant à lui, disponible uniquement pendant 60 jours.
- **Notification des failles de sécurité** et alerte des clients concernés dans les plus brefs délais afin qu'ils puissent réagir rapidement en tant que responsable des traitements.
- Hébergement des données et serveurs sécurisés :
 - L'ensemble des **données sensibles / données clients** :
 - Sont stockées sur un SAN (Storage Area Network) via un réseau interne dédié en fibre optique qui bénéficie d'une maintenance préventive plusieurs fois par an.
 - Les serveurs SQL hébergeant les données de nos clients sont donc uniquement connectés sur le réseau interne : ils ne sont donc pas accessibles depuis l'extérieur, ce qui leur garantit une protection totale.
 - Les serveurs SQL sont des serveurs physiques afin de garantir le plus haut niveau de sécurité et de performance.

- Hébergées dans un cadre contractuel de stricte confidentialité, les données de nos clients sont isolées et sauvegardées quotidiennement (cryptage en cours).
- Seuls les **serveurs d'envois e-mails et web** sont connectés sur l'extérieur :
 - Ils sont protégés par Firewall et l'insertion des données est contrôlée par des scripts développés en interne.
 - Les serveurs applicatifs hébergés sont sur une plateforme virtuelle dans notre propre infrastructure (Cloud privé).
 - Architecture en haute disponibilité avec des serveurs redondés et avec une répartition de charge automatique.
 - Maintenance proactive et préventive régulière des serveurs, logiciels, espaces disques, etc.
- Hébergement de l'infrastructure technique dans un **Data Center français** dont l'accès est sécurisé et limité au personnel habilité :
 - La plateforme technique de DOLIST est hébergée en salle blanche privée.
 - Le Data Center correspond à une classification équivalente TIER III+.
 - Sécurité Anti-intrusion
 - Systèmes de vidéosurveillance afin de surveiller et superviser en temps réel les espaces d'hébergement et zones d'accès.
 - Personnel de surveillance (sécurité et incendie) sur place 24h/24 7j/7.
 - Sécurité anti-incendie.
 - Continuité de la production électrique avec des circuits internes redondés.
 - Continuité de la chaîne de refroidissement.
 - Accès limité au personnel habilité.
- Réseau redondé sur 2 opérateurs télécom.
 - Utilisation du protocole BGP4 qui permet un routage dynamique sur nos 2 opérateurs et assure une haute disponibilité du transit IP.
 - DOLIST est membre du RIPE et donc propriétaire de ses adresses IP (cela nous confère une indépendance vis-à-vis de nos fournisseurs de transit IP).
 - Protégé par des pare-feux redondants.
 - Système de protection anti-DDOS (attaque par déni de service).
- Sauvegarde des données et des systèmes :
 - Sauvegarde via un réseau local dédié.
 - Fréquence de sauvegarde pour les bases de données.
 - Sauvegarde tous les jours à minuit.
 - Sauvegarde différentielle toutes les 4 heures.

- Rétention sur 15 jours des sauvegardes différentielles.
- Copie mensuelle archivée avec une rétention de 4 mois.
- Fréquence de sauvegarde des systèmes d'exploitation et autres données.
 - Sauvegarde complète tous les jours à minuit.
 - Rétention sur 15 jours.
- Chaque semaine, un jeu de sauvegarde est déposé dans un coffre ignifugé sur un autre site distant.
- Des procédures de sécurité internes complémentaires :
 - Supervision permanente des plateformes marketing Dolist 24h/24 et 7j/7.
 - Remontée d'alertes par SMS auprès de plusieurs ingénieurs en cas d'incidents.
 - Contrats de maintenance matérielle avec GTR 4h.
 - Monitoring en temps réel des Blacklists de domaines et d'adresses IP.
 - Suivi et contrôle de la qualité des fichiers chargés grâce à des alertes en cas d'anomalie.
 - Monitoring des accès aux plateformes marketing Dolist.
 - Maintenance proactive et préventive des serveurs, logiciels, espaces disques...
 - Sauvegardes quotidiennes effectuées sur des NAS de plusieurs téraoctets.
 - Contrôle permanent de la disponibilité des plateformes marketing Dolist.

Mise en conformité RGPD & Accompagnement de nos clients

- Des **solutions technologiques** accompagnent nos clients pour :
 - Une collecte opt-in des contacts, preuve des consentements à l'appui.
 - Une durée conservation des données paramétrable selon les instructions du client, en accord avec le RGPD.
 - Des mécanismes qui assurent le respect des droits aux personnes de manière explicite, y compris le désabonnement, dont les adresses e-mail sont uniquement conservées à des fins d'exclusions des envois et dont les données personnelles rattachées sont anonymisées.
- Depuis 2009, de multiples services complémentaires pour :
 - Auditer et optimiser la qualité des bases de données.
 - Former aux bonnes pratiques de collecte de contacts.

- Conseiller et accompagner au déploiement de stratégies marketing plus déontologiques et durables.
- **Sensibilisation permanente** de nos clients aux bonnes pratiques Marketing et aux bénéfices d'une approche déontologique via des conférences, webinars, livres blancs, articles sur notre blog d'information, newsletters...
- **Accréditation Dolist** des clients justifiant leur respect de la législation en matière de base de données et l'hygiène de leur base de contacts.

Protection des droits & information des personnes (en tant que responsable de traitement)

- **Mise à jour notre politique de confidentialité/mentions légales**, notamment en matière d'utilisation des données personnelles et la rendre le plus accessible possible.
- **Valorisation de notre charte de protection des données personnelles** et de gestion des cookies (définition, usage, désactivation des cookies, durée de conservation, droits d'accès/d'opposition).
- **Recueil du consentement** des individus pour la collecte de données personnelles et comportementales (cookies) via une action explicite du contact et en conserver la preuve.
- **Information des personnes en toute transparence** sur tous les formulaires de collecte et dans les mentions légales du site, sur l'ensemble des conditions de traitement des données, en conformité avec l'article 13 du RGPD.
- En plus des droits d'accès, de correction et de suppression des données, mise en place d'un **droit à l'effacement des données** (droit à l'oubli numérique).
- **Respect des grands principes liés au traitement des données personnelles** (licéité, loyauté, transparence, limitation des finalités, limitation de conservation, minimisation, exactitude, intégrité et confidentialité des données) et être en mesure de démontrer, à tout moment, leur respect.
- **Limitation de l'utilisation des données personnelles dans un objectif de profilage** aux seuls besoins d'analyse de performance, d'amélioration de la connaissance client et de personnalisation des échanges.
- La **gestion et le traitement des données** sont réalisés **en Europe**, hors dérogations spécifiques.
- Ne jamais vendre, partager ou louer les données personnelles.

A propos de Dolist

Créée en 2000, Dolist propose des **solutions SaaS de routage & de conception e-mail/SMS**, sécurisées, compatibles RGPD et "made in France" :

- **Campaign** : la plateforme d'activation e-mail/SMS pour tous les types d'envoi : transactionnels, marketing, automation, notifications.
- **Welkom Editor** : un email builder collaboratif pour la conception de messages optimisés Responsive, délivrabilité et accessibilité.

Dolist propose en parallèle des **services d'accompagnement spécialisés** : connectivité API/Data, délivrabilité, Studio Tech & Design, conseil, numérique responsable, formations, Customer Success Management.

Dolist intervient aussi sur les **plateformes standards du marché** : Salesforce Marketing Cloud, Pardot, Adobe Campaign, Hubspot...

L'ensemble de ses solutions vise à guider ses clients vers **une communication responsable, inclusive et pertinente**.

Informations et actualités : www.dolist.com

Contactez-nous

Standard : +33 (0)5 57 26 25 70

E-mail : info@dolist.com

Pour toute question relative à la protection des données traitées par Dolist pour son propre compte (responsable de traitement), vous pouvez contacter notre DPO : dpo@dolist.com