edipub

facilitateur de business

Guide EdiPub

Comprendre et appliquer la RGDP

« Protection des données personnelles »

Règlement Européen applicable au 25 mai 2018

SOMMAIRE

OBJECTIFS DU DOCUMENT

A la demande de ses adhérents, EdiPub reprend dans ce document une série de recommandations afin d'aider chacun de ses membres à **répondre aux nouvelles exigences édictées par le Règlement Européen en matière de droit des individus sur leurs données personnelles**.

Prenant en compte l'évolution des technologies digitales et des pratiques du marché, la Loi d'Harmonisation Européenne (27 pays) impose des responsabilités nouvelles aux entreprises amenées à collecter, traiter, regrouper et analyser des données personnelles et comportementales.
Il s'agit de protéger les consommateurs et de leur redonner de la confiance dans les relations avec les entreprises.
Tous les acteurs impliqués dans le traitement des données engagent leur responsabilité *(et non plus seulement le responsable du traitement, comme c'était le cas jusqu'alors)*.
L'application de ce règlement est fixée au **25 mai 2018** et les sanctions infligées par les autorités de contrôle sont conséquentes, puisqu'elles peuvent aller jusqu'à 20 millions d'Euros ou **4% du chiffre annuel mondial**.
Au-delà du préjudice financier, l'entreprise met également en jeu sa réputation et sa crédibilité, et risque de dégrader fortement son image en cas de défaillance avérée.

Il convient donc de se préparer à cette mise en conformité ; *le secteur de la Publicité, au fait des techniques de ciblage et de profilage, est un secteur privilégié pour les instances de contrôle.*

COMMENT VOUS-Y PREPARER ?

Vous trouverez ci-dessous une check-list proposée conjointement par

- le ***cabinet « HAAS Avocats »***, spécialisé dans les questions de protection des données personnelles
- et « ***DoList*** » un prestataire de solutions Data & Messaging, connu pour ses solutions centrées sur la qualité des données, la délivrabilité des campagnes et l'optimisation de la stratégie e-mail marketing.

Réf : E-Marketing & Protection des données Nouvelle réglementation : Préparez-vous dès maintenant !

PROTECTION DES DROITS A LA PERSONNE

◁ Recueillir le consentement des individus pour la collecte de données comportementales (cookies) via une action positive et explicite du contact *(exemple : case à cocher)* et en conserver la preuve.

◁ Limiter la collecte des données au strict minimum requis pour l'accomplissement d'un objectif *(principe de minimisation)*.

◁ Respecter les grands principes liés au traitement des données *(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. **(« accountability »).**

◁ Prendre en compte que, pour les contacts de moins de 16 ans, leur consentement n'est valable que s'il est accordé par leur responsable légal.

◁ S'assurer que l'utilisation des données dans un objectif de profilage ne soit pas discriminante *(basée notamment sur l'origine, l'orientation sexuelle, l'état de santé, les opinons politiques, religieuses ou syndicales)*.

◁ En plus des droits d'accès, de correction et de suppression des données, mettre en place un droit à l'effacement des données **(« droit à l'oubli numérique »)**.

◁ Assurer le transfert des données à un tiers dès lors que la personne concernée par le traitement le réclame (**droit de portabilité**).

◁ S'assurer que la gestion et le traitement des données se réalisent dans le cadre des frontières européennes, hors dérogations spécifiques.

◁ Ne pas vendre, partager ou louer les données personnelles, hors consentement explicite des contacts.

INFORMATIONS AUX PERSONNES

◁ Expliquer clairement quelles sont les informations collectées, cédées, partagées sur les formulaires d'inscription et dans les mentions légales du site. Mentionner également les raisons de leur collecte.

◁ Lister les données personnelles détenues précisant leur sensibilité, source, caractère obligatoire ou non, les destinataires *(y compris hors UE)* et leur durée de conservation.

◁ Répertorier tous les traitements de l'entreprise faisant intervenir des données personnelles *(par exemple la collecte, conservation, modification, utilisation, diffusion, etc.)*.

◁ Définir la politique de confidentialité/mentions légales de l'entreprise, notamment en matière d'utilisation des données personnelles.

◁ Rendre accessible la politique de confidentialité/mentions légales depuis tous les modes de collecte *(formulaires notamment)* et depuis la page d'accueil du site.

◁ Mettre en place la Charte de Protection des Données Personnelles et de gestion des cookies *(définition, usage, désactivation des cookies, durée de conservation, droits d'accès/d'opposition)* et la valoriser sur le(s) site(s) de l'entreprise.

◁ Fournir les détails de la collecte d'un contact sur demande *(date, adresse IP, mode de collecte, etc.)*.

OBLIGATIONS DE SECURITE & D'ANTICIPATION DES RISQUES

◁ S'assurer que les prestataires ayant accès aux données ou en lien avec la gestion des données respectent les obligations de sécurité et de protection des données.

◁ Réaliser une étude d'impact sur la vie privée **(« Privacy Impact Assessment » - PIA)** permettant d'évaluer l'adéquation des mesures prises par le responsable de traitement au regard des risques encourus sur la vie privée.

◁ Garantir que, par défaut, seules les données qui sont nécessaires au regard de la finalité de chaque traitement, sont traitées : limiter la quantité de données collectées, anonymiser les données, limiter la durée de conservation, etc…
(« Privacy by default »)

◁ Nommer un **« Data Privacy Officer » (DPO)** si :

- L'entreprise ou le sous-traitant appartient au secteur public
- L'activité principale amène à réaliser un suivi régulier et systématique des personnes à grande échelle

 L'activité principale implique un traitement à grande échelle des données sensibles *(origine, santé, orientation sexuelle, opinion politique etc.)* ou relatives à des condamnations.
Le DPO est en charge de la protection des données, de la sensibilisation des collaborateurs de l'entreprise et du suivi de l'évolution du traitement des données. Gérant les dimensions techniques, réglementaires et la mesure du risque, il doit tout mettre en œuvre pour mettre et maintenir l'entreprise en conformité.

◁ **Mettre en place un registre des traitements des données pour l'entreprise** et ses sous-traitants avec une liste des mesures précisant :
- le nom,
- les coordonnées du responsable ou du DPO,
- la finalité,
- les personnes concernées,
- les destinataires,
- les transferts de données hors UE,
- les délais prévus pour l'effacement des données,
- la description des mesures de sécurité mises en place.

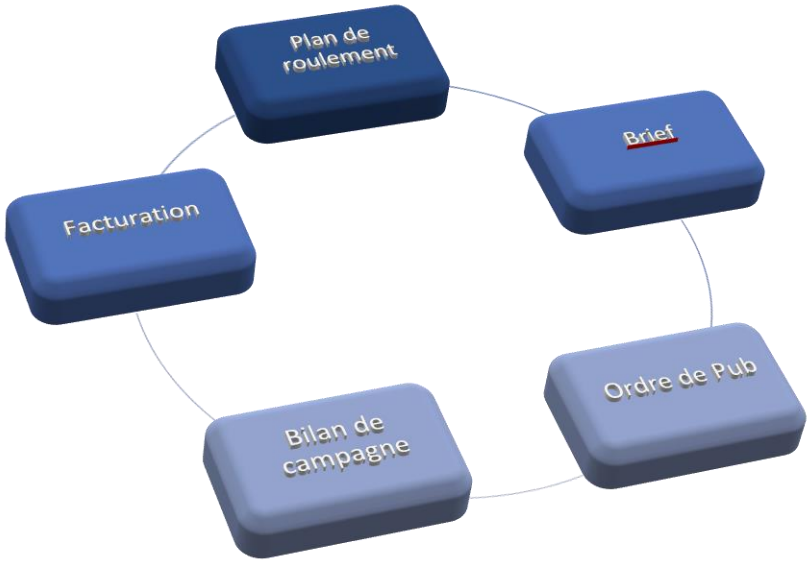
◁ **Réaliser régulièrement des tests techniques d'intrusion** / accès aux données avec tenue d'un registre des incidents de sécurité détaillés.

◁ **Ajouter dans les contrats de sous-traitance une clause imposant un audit de sécurité.**

◁ Sensibiliser le personnel aux enjeux de confidentialité et de sécurité des données.

RECOMMANDATIONS SUR LE PERIMETRE EDIPUB

Un groupe de travail s'est réuni, sous l'égide d'EdiPub, pour définir les recommandations relatives aux données personnelles intervenant dans les processus métier **dans le périmètre des échanges EDI**.
Il a été convenu que les autres processus métier, hors périmètre actuel d'EdiPub, ne seraient pas traités dans ce document.



Dans le périmètre EdiPub schématisé ci-dessus, les seules données personnelles qui transitent dans les échanges EDI sont **des informations d'identification des acteurs du processus** dans les organisations professionnelles ; *par exemple :*

- L'interlocuteur dans le service ADV de la régie,
- L'acheteur en agence média, le responsable planning en régie
- Les collaborateurs en charge de la facturation,
- …

Ces informations transitent de **manière optionnelle** et si elles sont renseignées, le message EDI véhicule 4 informations :

- Un nom
- Une adresse email *(souvent professionnelle)*
- Un n° de téléphone (souvent professionnel)
- Un n° de fax

Aujourd'hui, aucune information relative aux clients finaux ne transite dans les échanges EDI.

Au regard des obligations énumérées dans le chapitre précédent, EdiPub préconise le process suivant :

- ➔ IDENTIFIER LES INTERLOCUTEURS, NON PLUS INDIVIDUELLEMENT, MAIS PLUTOT PAR DES ENTITES ORGANISATIONNELLES, DES SERVICES DANS L'ENTREPRISE, AFIN D'**ANONYMISER CES CONTACTS**
- ➔ **UTILISER DES ADRESSES EMAIL GENERIQUES PAR SERVICE OU PAR BU par exemple**, PLUTOT QUE DES ADRESSES CONTENANT LE NOM ET LE PRENOM DE L'INDIVIDU, MEME QUAND CE SONT DES ADRESSES PROFESSIONNELLES.

Cette solution permettrait purement et simplement de se dégager de toute contrainte sur les données personnelles dans le cadre strict des échanges EDI.

Néanmoins, du point de vue de la confidentialité et de la sécurité, les enjeux restent les mêmes. Les données des bons de commandes, factures, bilans de campagne sont considérées comme confidentielles par rapport à l'activité et ne doivent en aucun cas être accessibles aux personnes non habilitées.

Si les préconisations / recommandations formulées ci-dessus par EdiPub se limitent au périmètre indiqué précédemment, il est certain que les obligations légales vont bien au-delà pour les agences média, les éditeurs et les régies publicitaires, qui exploitent quotidiennement les données clients :

- *Pour vendre ou acheter de l'espace publicitaire*
- *Pour optimiser les campagnes avec des techniques de ciblages et de profilage (avec stockage IP sur des sites publics par exemple) ;*
- *Pour développer les ventes basées sur l'audience et les cibles garanties*
- *…*

Il appartiendra alors à chaque entreprise :

- ➔ D'ETENDRE LA MISE EN CONFORMITE A L'ENSEMBLE DES TRAITEMENTS CONCERNES PAR DES DONNEES PERSONNELLES ET A REPONDRE AUX OBLIGATIONS DE DECLARATIONS IMPOSEES (DECLARATION DES TRAITEMENTS ET DE LEUR FINALITE). CI-DESSOUS LE REGISTRE PROPOSE PAR LA CNIL

registre-reglement-publie.xlsx

- ➔ DE REVISER L'ENSEMBLE DES CONTRATS AVEC SES PARTENAIRES (PRESTATAIRES INFORMATIQUES ET METIER), POUR LES OBLIGER A UNE MISE EN CONFORMITE, EVENTUELLEMENT LEUR EN DEMANDER LA PREUVE A FREQUENCE REGULIERE, POUR **REDUIRE L'EXPOSITION AU RISQUE** INDUITE PAR L'INTRODUCTION DE CLAUSES DE CORESPONSABILITE DANS LES TEXTES.

OBLIGATIONS EDIPUB SUR LES DONNEES PERSONNELLES DE SES ADHERENTS

EdiPub propose un **portail d'échanges collaboratifs** qui permet le partage d'informations et la communication avec ses adhérents.
Ce portail conserve des données à caractère personnel et à ce titre, EdiPub est directement concerné par l'application des principes et des règles régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Le règlement impose la tenue d'une documentation interne, décrivant les traitements de données personnelles, leur finalité, et leur conformité par rapport aux nouvelles obligations légales.

Pour remplir ces obligations, EdiPub a recensé :

- Les données personnelles traitées
- Les différents traitements associés
- Les objectifs poursuivis par ces traitements
- Les acteurs qui traitent ces données, les sous-traitants intervenant dans leur gestion
- Les flux d'information

(voir chapitre Registre des traitements EdiPub, ci-après).

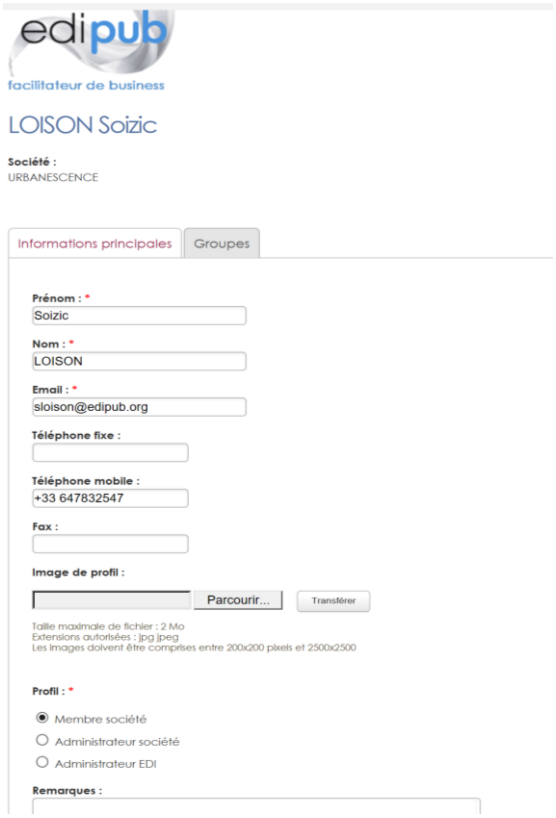
REGISTRE DES TRAITEMENTS EDIPUB

LES DONNEES PERSONNELLES

RECENSEMENT DES DONNEES PERSONNELLES

Les données personnelles des adhérents d'EdiPub sont gérées au niveau des utilisateurs de la société.

La fiche utilisateur contient les informations suivantes, lesquelles constituent évidemment des données à caractère personnel.



Dans le chapitre suivant, nous expliciterons précisément la finalité des traitements de ces données personnelles.

LES DOCUMENTS PUBLIES

Le nom et les coordonnées d'un contact peuvent apparaitre dans certains documents publiés sur le site.
Ces documents sont publiés dans la majorité des cas en version PDF et les données ne sont pas directement exploitables par des outils informatiques.

Pour les documents, le site dispose d'un moteur de recherche indexant les fichiers joints (PDF) ; **ce moteur de recherche prend en compte les droits d'accès**.
Ainsi un fichier PDF de l'extranet ne peut être trouvé et consulté, que par un membre de l'extranet.
Si ce fichier est publié dans un groupe de travail, seul les membres de ce groupe y ont accès.

LES COMMENTAIRES

Le site propose des fonctionnalités permettant à un utilisateur d'émettre des commentaires sur un document.
Quand un utilisateur n'est pas connecté, il indique sous quel nom son commentaire doit être posté. Il est donc consentant à ce stade sur la publication de ces informations.

Quand un utilisateur adhérent EdiPub est connecté, ses commentaires sont forcément publiés en son nom et il apparaît clairement comme auteur du commentaire.
Dans la partie extranet, cet utilisateur ne peut donc pas publier « anonymement ». Il peut en revanche le faire dans la partie publique, en se déconnectant avant de laisser un commentaire.

➔ VU AVEC L'HEBERGEUR DU SITE (PLUME) : NOUS POURRONS PROPOSER UNE FONCTION DE SUPPRESSION DE SES PROPRES COMMENTAIRES A CHAQUE UTILISATEUR AYANT UN COMPTE SUR LE SITE.

REPONSE A L'OBLIGATION DE CONSENTEMENT DES PERSONNES

Sur le site « edipub.org , il existe 4 types de profils :

- Le visiteur
- L'utilisateur
- Le super-utilisateur société (qui dispose de droits de gestion des utilisateurs de sa société)
- L'administrateur EDI (qui dispose de droits de gestion de l'ensemble des utilisateurs)

Un compte utilisateur est créé sur le site par l'administrateur EDI du site ou le super-utilisateur de la société d'appartenance de l'utilisateur.
Dans tous les cas, l'un ou l'autre doit s'assurer du consentement de l'utilisateur à la création de son compte et l'information de ses données personnelles.

D'après les textes, il conviendrait de conserver la preuve de ce consentement.
Actuellement le site ne demande pas ce consentement, et n'en conserve pas la preuve.

➔ VU AVEC L'HEBERGEUR DU SITE (PLUME) : NOUS POURRONS RECUPERER LE CONSENTEMENT RELATIF A UNE CREATION DE COMPTE PAR UN ENVOI DE MAIL A L'UTILISATEUR QUI VALIDERA L'ACTIVATION DE SON COMPTE (CE QUI VAUDRA CONSENTEMENT).

Remarques :

- seul un utilisateur dispose d'un accès à son compte personnel ; le super-utilisateur peut simplement créer/modifier/supprimer le compte mais il ne peut pas l'utiliser
- Un super-utilisateur d'une société dispose de tous les droits sur le compte d'un utilisateur de sa société : il peut modifier ses informations personnelles sans que l'utilisateur ne le sache ou le valide.

REPONSE A L'OBLIGATION DE PERTINENCE DES DONNEES

Les textes prônent le **« principe de minimisation »** de la collecte ; en d'autres termes, seules les données strictement nécessaires à la réalisation de l'objectif peuvent être collectées.

Par ailleurs, des mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées, soient effacées ou rectifiées.

L'extranet EdiPub répond à ces obligations :

- « Minimisation de la collecte » : nous verrons dans le chapitre sur la finalité des traitements que l'objectif principal de la collecte de ces données est l'envoi de notification et la mise à disposition d'un annuaire des adhérents de l'association, dont la diffusion est restreinte aux membres de la communauté EdiPub. Les informations « nom, prénom, email », sont à ce titre nécessaires et suffisantes ; l'information du n° de téléphone / fax est optionnelle *(seules les données : « nom, prénom, email », sont obligatoires)*.

- ***Visibilité des identités et informations personnelles :***
    - **Sur la partie publique du site** :
        - Les noms des super-utilisateurs des sociétés sont visibles : c'est un fonctionnement automatique. Le site ne demande pas à chaque super-utilisateur s'il accepte cet affichage.
        - Aucun mail ou information personnelle (autre que les noms des super-utilisateurs dans l'annuaire des sociétés) n'est visible sur la partie publique.

    - **Sur la partie privée du site** :
        - Un utilisateur connecté peut voir toutes les informations des autres utilisateurs car il a accès à leur fiche (nom, prénom, mail, société, téléphone, fax).
        - Un utilisateur ne peut pas choisir de ne pas être visible dans l'annuaire ou de ne pas permettre de consulter sa fiche aux autres utilisateurs.
        - Mais il peut demander à être retiré du site *(voir ci-après)*

- Effacement et rectification : un utilisateur inscrit sur le site EdiPub a toute latitude pour modifier l'ensemble de ses données personnelles. S'il désire « effacer » son compte utilisateur, il en fera une demande à l'administrateur du site au sein d'EdiPub (contact@edipub.org) ou au super-utilisateur de sa société.

CONSERVATION

Le Règlement Européen exige que les données à caractère personnel soient conservées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

Une fois que l'objectif poursuivi par la collecte des données est atteint, il n'y a plus lieu de les conserver et elles doivent être supprimées.

L'extranet EdiPub répond à ces obligations en mettant à disposition de l'utilisateur :

- des fonctionnalités de modification de ses données personnelles
- une procédure de demande de suppression, passant soit par un administrateur de sa société (super-utilisateur), soit par les correspondants au sein de l'association EdiPub (administrateur EDI).

Les données supprimées ne sont pas archivées. Le compte est entièrement et définitivement supprimé, et toutes les données personnelles effacées *(« droit à l'oubli numérique »))*.

Rq : ne pas confondre avec le « blocage » d'un compte : dans ce cas on conserve tout, avec la possibilité de réactivation du compte.

Les envois de mail sont historisés dans les logs du site pendant un temps limité, (environ une semaine), à des fins de surveillance du bon fonctionnement du processus d'envoi ; ensuite ils sont effacés.

TRAITEMENTS, FINALITE DES TRAITEMENTS SUR CES DONNEES PERSONNELLES ET ACTEURS INTERVENANTS DANS LE TRAITEMENT

Les données suscitées sont collectées pour des finalités bien déterminées.

Les traitements de données personnelles identifiés dans le périmètre EdiPub sont les suivants :

- **T1** : Notifier automatiquement les utilisateurs de la mise à disposition d'un document ou d'une information
- **T2** : Diffuser de l'information à un groupe d'utilisateurs rattachés à un groupe de travail
- **T3** : Forcer l'envoi de notification
- **T4** : Envoyer un mail groupé

La finalité de chacun des traitements est indiquée ci-après :

- **T1 : Notifier automatiquement les utilisateurs de la mise à disposition d'un document ou d'une information**

Lors de la publication d'un document ou d'un rendez-vous dans un groupe de travail, un message est automatiquement envoyé aux membres du (des) groupe(s) en question, comportant un lien vers l'article du site et, le cas échéant, vers le document qui lui est attaché.

- **T2 : Diffuser de l'information à un groupe d'utilisateurs rattachés à un groupe de travail**

Chaque groupe de travail dispose d'une fonction de liste de diffusion permettant aux administrateurs EDI d'envoyer un message à tous les utilisateurs inscrits à ce groupe.

- **T3 : Forcer l'envoi de notification**

Par défaut, tout membre d'un groupe reçoit des notifications de ce groupe, mais un utilisateur peut cocher une case dans son profil pour ne pas recevoir ces notifications... Malgré tout, les administrateurs EDI du site peuvent tout de même forcer une notification importante pour que tout le monde la reçoive *(même ceux qui ont coché la case)*.

- **T4 : Envoyer un mail groupé**

Les administrateurs EDI du site peuvent envoyer un mail depuis l'annuaire du site.
Les utilisateurs ne peuvent pas choisir d'être exclus de ces envois aujourd'hui.

RESPECT DES DROITS DES PERSONNES ET OBLIGATION D'INFORMATION

Des données concernant des personnes peuvent être collectées à la condition essentielle qu'elles aient été informées de cette opération.

➔ LE RESPONSABLE DE TRAITEMENT DOIT PRECISEMENT ANNONCER AUX PERSONNES CONCERNEES A QUOI VA SERVIR LE RECUEIL DE DONNEES, & S'ENGAGER SUR LA MANIERE DONT IL POURRA UTILISER OU REUTILISER CES DONNEES DANS LE FUTUR.
➔ IL DOIT REDIGER DES COMMUNICATIONS DANS CE SENS…

OBLIGATIONS DE SECURITE & D'ANTICIPATION DES RISQUES

Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Cette obligation est totalement assurée par la sécurisation du site et du serveur (hébergeur)...

Attention : vu avec l'hébergeur du site : le site est en Drupal 6 qui n'est plus maintenu par la communauté donc le risque de faille existe même si cela n'est jamais arrivé jusqu'ici. Un passage à la dernière version du CMS signifierait une meilleure sécurité.
Ce passage a été acté au Conseil d'Administration EdiPub du 15 juin 2017, et la mise en conformité du site EdiPub.org avec le Règlement Européen sur les Données Personnelles sera effective avec le changement de version.

EDIPUB A VOTRE SERVICE

Edi Pub se tient à votre disposition pour vous accompagner dans la mise en conformité de la réglementation applicable à la protection des données.

Nous pouvons ensemble identifier les forces et les faiblesses de vos pratiques et identifier les leviers de progression.

Contactez-nous :

- **Evelyne Sosnovsky** *esosnovsky@edipub.org*
- **Soizic Loison** *sloison@edipub.org*