RGPD

Principes et mise en œuvre

bedood

PRÉFACE

À quelques mois de l'entrée en application du Règlement Général sur la Protection des Données (RGPD), les professionnels doivent concentrer leurs actions sur la mise en conformité aux nouvelles règles applicables à partir du 25 mai 2018.

Ce nouveau règlement est complexe et ceux ne le respectant pas s'exposent à des risques notables (amendes pouvant aller jusqu'à 20 million d'euros).

BeClood tend à aider à sa préparation et propose ainsi un récapitulatif des points clés du règlement en mettant à disposition les informations et pratiques essentielles aux professionnels du web afin de se préparer et de faire le point face à cette transition juridique.

Le RGPD entend avant tout responsabiliser les entreprises sur leurs utilisations des données personnelles des citoyens européens. À partir de son entrée en vigueur, ***le consentement des citoyens devra être obtenu par toute entreprise souhaitant utiliser leurs données****. Les entreprises devront, de plus, désigner de manière claire quelles seront* ***les utilisations faites des données****.*

Du côté des citoyens, ceux-ci pourront s'appuyer sur le règlement pour défendre leurs informations personnelles notamment s'ils estiment qu'une organisation les utilise de manière trop intrusive.

Le RGPD est une mise à jour de la directive européenne de 1995 et a été approuvé par 29 pays européens signataires. Elle prend en compte l'intégration des entreprises les plus influentes dans l'économie des données personnelles (celles du GAFA) et vise à harmoniser et protéger les droits des citoyens européens.

Le règlement établit des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données.

DONNÉES PERSONNELLES

Le règlement définit ainsi « *constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres …* ». Concrètement, il s'agit des données utilisables lors de l'identification d'une personne telles que :

- Nom, prénom,
- Numéro de téléphone,
- Numéro de sécurité sociale,
- Adresse électronique,
- Informations de paiement,
- Empreinte,
- Adresse IP,
- Pseudonyme,
- etc.

N.B. La loi distingue certaines données personnelles dites « sensibles » telles que les données génétiques ou biométriques, les opinions politiques, l'orientation sexuelle, l'origine ethnique ou l'appartenance religieuse.

CHAMPS D'APPLICATION

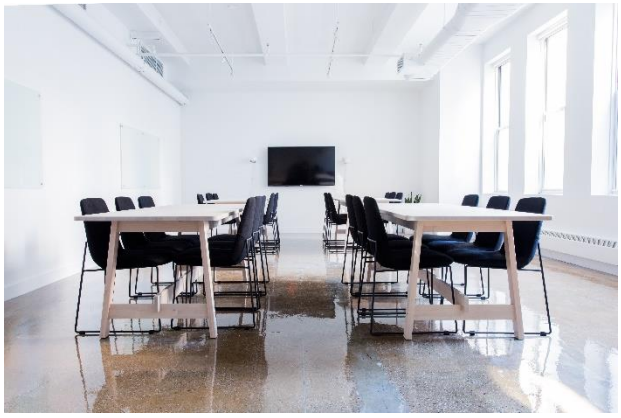
MATÉRIEL

Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en totalité ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

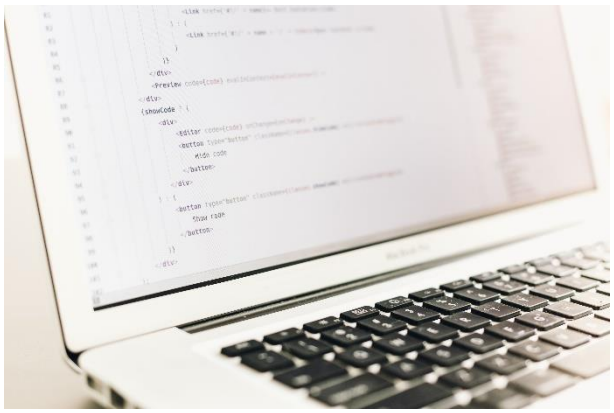
TERRITORIAL

Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement responsable du traitement.

LES PREMIERS PAS



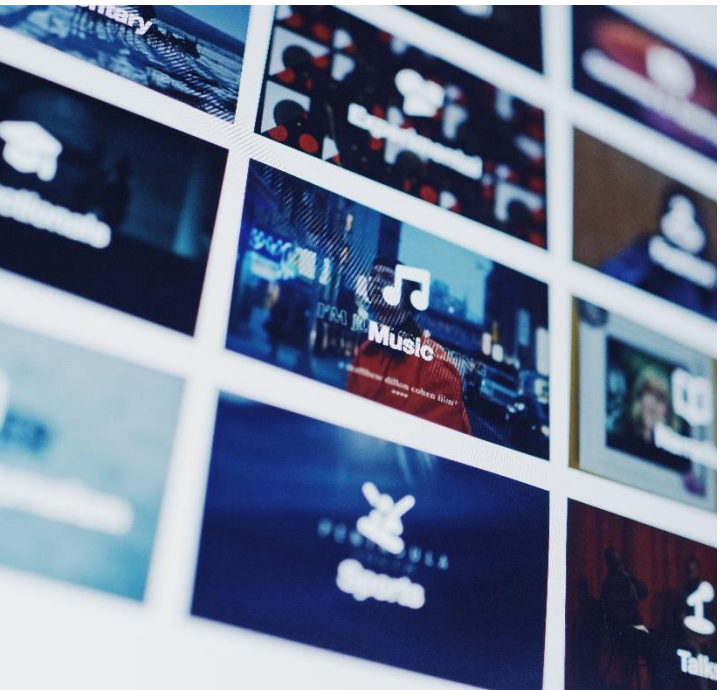
- ***Identifier**, connaître et suivre les données personnelles (inventaire des données),*
- *S'assurer de **la conformité** des données (opt-in, consentement),*
- ***Protéger** les données personnelles (droits d'accès, si des données personnelles sont présentes dans les bases de données, les supprimer ou les rendre anonymes…),*
- ***Partager** les données personnelles avec les personnes concernées.*



Si un utilisateur demande à accéder à ses données, la loi prévoit un délai de 25 jours pour donner accès aux informations. La personne concernée doit pouvoir consulter dans un même espace toutes ses données (CRM, base de données clients, tracking…). Elle doit pouvoir les rectifier, pouvoir user de son droit de portabilité, les exporter (JSON, XML, CSV…) et/ou exercer son droit à l'oubli et facilement faire une demande de suppression.

QUI EST CONCERNÉ ?

Toute entreprise ou organisme traitant des données personnelles provenant d'utilisateurs qui se trouvent ***dans l'Union Européenne****. Le RGPD concerne toutes les organisations y compris ceux qui n'ont pas d'activité sur Internet. Par exemple, une liste des salariés d'une société est aussi considérée comme un fichier de données personnelles.*



À noter qu'est concerné ***tout sous-traitant sur le territoire de l'Union****, que le traitement ait lieu ou non dans l'Union et à partir du moment où les activités de traitement sont liées à des personnes dans le territoire européen.*

Le non-respect de ce règlement entrainera ***des amendes pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires****.*

Le RGPD établit ainsi des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et des règles relatives à la libre circulation de ces données.

BIEN SE PRÉPARER

LES ÉTAPES RECOMMANDÉES PAR LA CNIL

01

Nommer un délégué à la protection des données personnelles

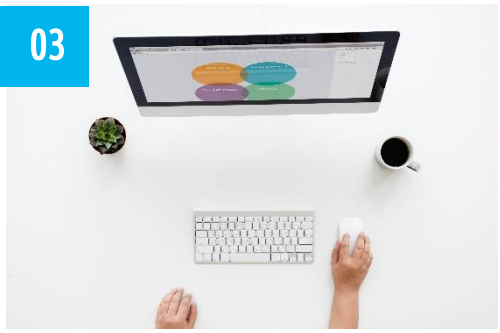
Obligatoire pour les grandes entreprises et organismes publics mais fortement recommandé pour tous.

Réaliser un registre de traitement des données

Répertorier tous les fichiers contenant des informations personnelles dans un registre de traitement et s'assurer que le consentement des citoyens y a été obtenu dans les règles.

02

03



Mettre en place une procédure

Toute entreprise ayant une activité sur Internet se doit d'effectuer un travail pour répondre aux futures réclamations portant sur le droit à l'oubli ou la portabilité des données.

Pour plus d'informations, cliquez ici

LES ESSENTIELS

POUR LES PROFESSIONNELS DU WEB

01. LE DIAGNOSTIC

La mise en place d'un diagnostic est nécessaire afin d'assurer la conformité de votre site web au nouveau règlement Européen. Les points clés sont listés ci-dessous :

- *Liste des données personnelles collectées (normales, sensibles),*
- *Liste des traitements effectués (action d'anonymisation ou de minimisation),*
- *Services externes utilisés,*
- *Gestion des cookies,*
- *Conformité du tracking (toute action de personnalisation doit mener à une étude d'impact),*
- *Conformité de l'hébergement (UE).*

DEMANDE ET ENREGISTREMENT DU CONSENTEMENT (OPT-IN)

02.

Le RGPD affiche que toute demande de consentement doit respecter les règles suivantes :

- *La demande de consentement doit être claire et concise, séparée de tout autre terme et/ou condition,*
- *Elle doit être libre, sans contraintes ni conséquences si refus,*
- *Si le consentement est une condition de l'inscription et/ou d'un téléchargement (par exemple), le consentement doit pouvoir être facilement prouvé,*
- *Doivent être inclus et lisibles :*
  - *Le nom de l'entreprise et de ses prestataires,*
  - *La finalité du traitement des données,*
  - *La procédure à suivre pour annuler un consentement et le droit de le retirer à tout moment.*
- *Concernant l'opt-in,* ***favoriser un double opt-in et ne pas utiliser de cases pré-cochées*** *ou de paramètres par défaut,*
- *L'entreprise recueillant les données doit garder une preuve de la façon dont elle obtient le consentement incluant :*
  - *Les données de l'individu,*
  - *La date d'obtention des données,*
  - *Le but du recueil,*
  - *L'e-mail de confirmation contenant ces informations est fortement recommandé.*
- *Introduire le « droit à l'oubli numérique » (cf. Article 17).*

Chapitre 2 - Article 7
Conditions applicables au consentement

03. LES COOKIES & LA GESTION DES SERVICES EXTERNES

*Aujourd'hui et en application de la directive européenne dite « paquet télécom », **les internautes doivent obligatoirement être informés et donner leur consentement à l'insertion de traceurs** (cookies). Ils doivent pouvoir choisir de ne pas être tracés lorsqu'ils visitent un site ou utilisent une application. Un bandeau d'information préalable se doit ainsi d'être affiché.*

Le RGPD et notamment la directive E-Privacy – qui doit être mise à jour et être appliquée en association avec le RGPD - *étoffe cette directive en précisant que **chaque cookie sera dorénavant considéré tel une donnée personnelle** et se devra d'en subir le même traitement.*

Devra donc être mis en place, au niveau du bandeau dédié et de manière explicite :

- ***Un choix de niveaux de confidentialité** à l'utilisateur, qui pourra ainsi refuser tous les cookies non-vitaux au fonctionnement du site web,*
- ***Une liste des services externes** avec la possibilité de personnaliser les autorisations (non obligatoire mais vivement recommandé).*

LES COOKIES

Un "cookie" est un fichier de taille limitée, généralement constitué de lettres et de chiffres, envoyé par le serveur internet au fichier cookie du navigateur, situé sur le disque dur de votre ordinateur.

Différents cookies sont utilisés pour améliorer l'interactivité et les services des sites web dont la personnalisation des données présentées. Il en existe plusieurs types :

- *Les cookies de fonctionnement, nécessaires au site web,*
- *Les cookies d'audience,*
- *Les cookies tiers. Il s'agit notamment des services externes proposés par des sites tiers. Parmi les plus courants peuvent être cités :*
  - *Des boutons de partage (Twitter et Facebook),*
  - *Des listes de tweets (Twitter),*
  - *Des vidéos diffusées sur le site (YouTube, Dailymotion),*
  - *Des présentations animées (Prezi).*

LA PAGE « POLITIQUE DE CONFIDENTIALITÉ »

04.

« Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. »

*Chapitre 3 - Article 12 - **transparence** des informations*

La mise en place d'une page « Politique de confidentialité » devient obligatoire. Elle se doit d'être séparée des Conditions Générales d'Utilisation et autres mentions légales du site. Elle doit permettre de fournir de manière claire et concise les informations suivantes :

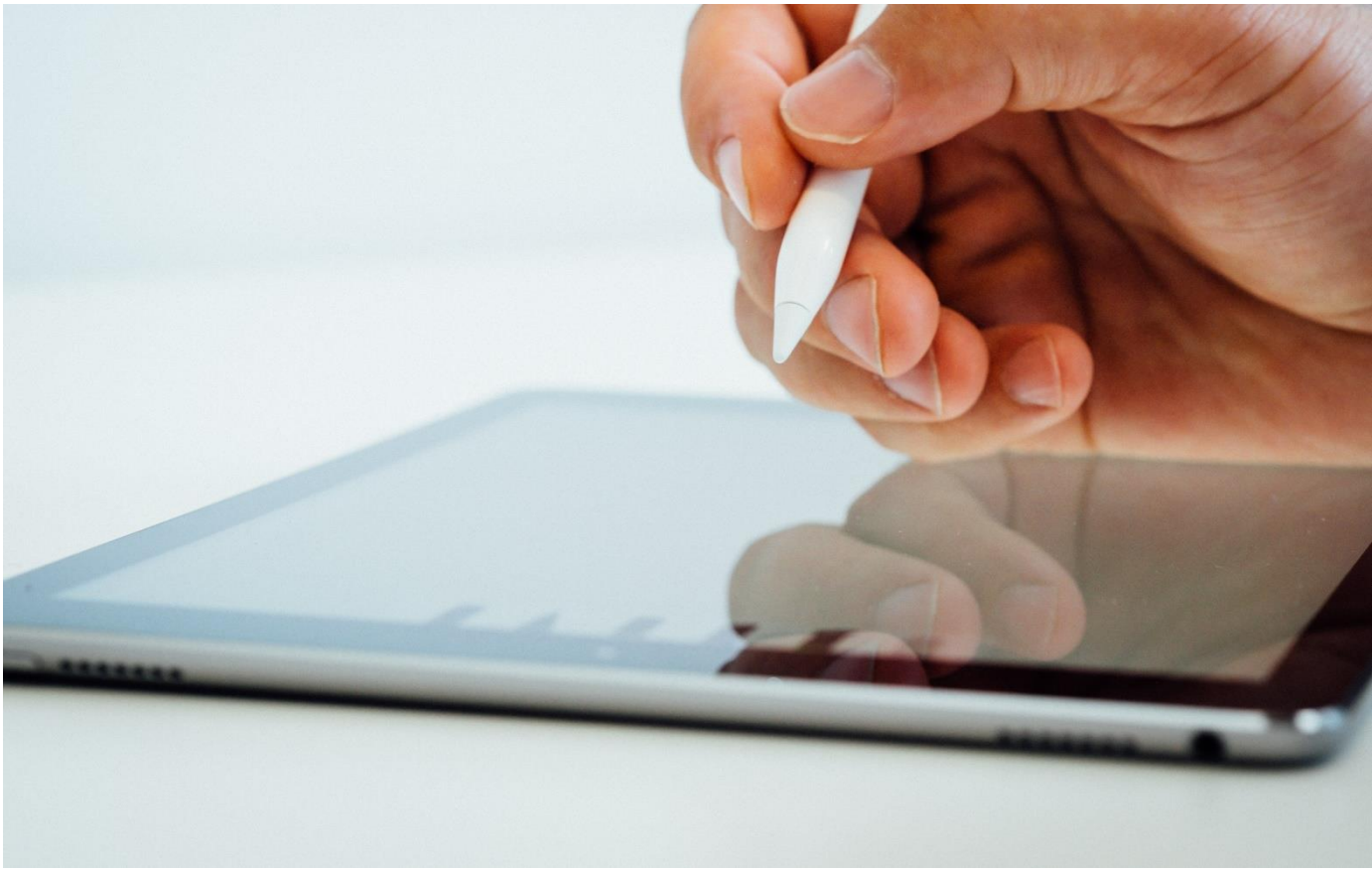
- *Le nom du responsable de traitement des données,*
- *La finalité du traitement des données,*
- *Les catégories de destinataires des données,*
- *Les droits d'accès, de rectification, d'opposition et suppression,*
- *Une mention du droit à la portabilité des données et de la possibilité de déposer plainte devant l'autorité compétente.*

Pour tout site web, cette page se devra d'apparaître en bas de toutes les pages (footer).

05. LES FORMULAIRES

Bien qu'un utilisateur puisse remplir et envoyer un formulaire de son plein gré le RGPD rend obligatoire et à afficher de manière claire et concise les éléments ci-dessous :

- *La durée de conversations des données,*
- *La finalité du traitement des données,*
- *La mention de conservation de l'adresse IP, ou non,*
- *Une demande de consentement,*
- *Le temps de conservation des données (peut aussi être indiqué dans la page « Politique de confidentialité »)*



À PROPOS

BeClood est une société d'ingénierie digitale créée en 2014 par 4 co-fondateurs dont l'expérience a été bâtie dans les sociétés leader de l'intégration de solutions ***Open Source****.*

Spécialistes ***eZ Platform*** *et* ***Symfony****, nous participons à la conception et au développement de vos projets digitaux.*

Aujourd'hui composée de 10 personnes, BeClood est une structure en pleine croissance dans un environnement jeune, tech et stimulant.

Pour vous aider à préparer votre transition au RGPD, BeClood vous accompagne et vous conseille. N'hésitez pas à nous contacter !

CONTACT

BeClood
Espace French Tech
1, place Francis Ponge
34000 Montpellier

marketing@beclood.com

Tél. : 09 72 42 26 03
Fax : 09 57 35 00 06