BOOSTACOM
communication · digital · formation web
www.boostacom.fr

FRANÇOISE SILVAN
AVOCAT MEDIATEUR

Petit-déjeuner conférence

RGPD : êtes-vous prêt ?

L'une des plus grandes réformes relatives au traitement des données personnelles par l'entreprise.

Présentation
des intervenants

FRANÇOISE SILVAN

« RÉTABLIR LE DIALOGUE,
ANTICIPER ET RÉGLER LES DIFFÉRENDS
POUR AMÉLIORER
LA PERFORMANCE EN ENTREPRISE. »

FRANÇOISE
SILVAN
AVOCAT
MEDIATEUR

04 75 80 55 40
06 07 21 54 03

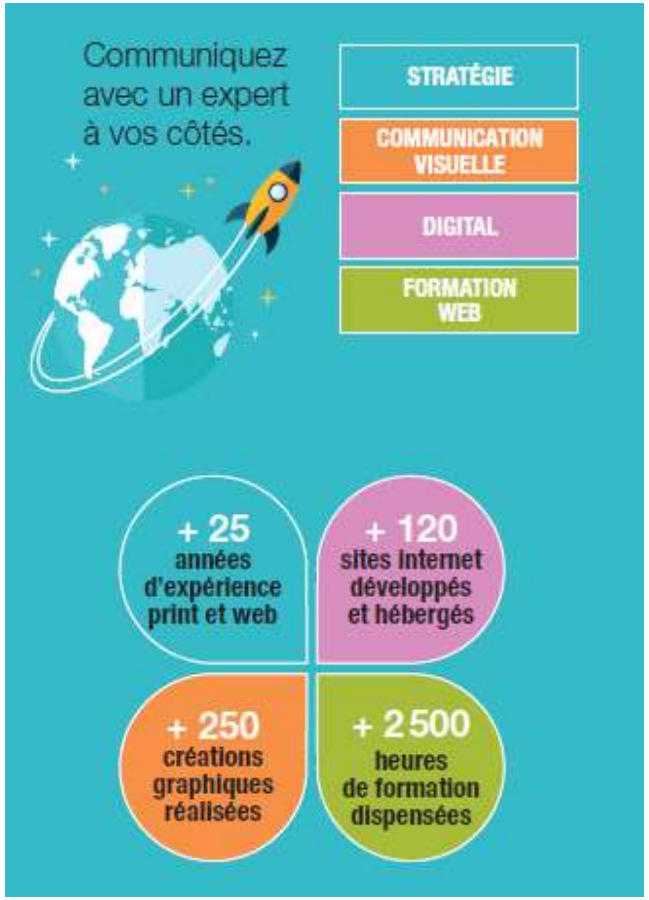
fs@silvan-avocat-mediateur.fr
21 rue Paul-Henri Spaak - 26000 Valence

www.silvan-avocat-mediateur.fr

BOOSTACOM

communication · digital · formation web

www.boostacom.fr



250 chemin de Seillères – 38160 Chatte
Tel 06 26 94 14 19 – c.tabarin@boostacom.fr

Contexte du RGPD

A l'ère du big data, nécessité de réglementer

- **Encadrer une pratique qui est devenue courante dans les usages :** stockage de données, informations personnelles sur les formulaires, réseaux sociaux (Facebook), publicité digitale…
- **Limiter l'achat et la revente de données sans consentement clair**

- **Mettre tous les pays européens au même niveau,** avec une réglementation européenne commune

Rappel législatif

AVANT

Loi du 6 janvier 1978
dite « Loi informatique et libertés » :
Pose les principes :
. Préservation de la sécurité des données
. Déclarations et autorisations préalables

La Charte des droits fondamentaux de l'Union européenne (Proclamée le 7/12/2000 et adoptée le 12/12/2007) :
La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental. (article 8)

AUJOURD'HUI

RGPD – 99 articles
Règlement Général sur
la Protection des Données

Règlement européen 216/679 du 27 avril 2016 sur la protection des données : applicable le 25 mai 2018
. Droits des citoyens renforcés
. Conformité en continue
. Avoir un niveau de sécurité adapté au risque

- **A partir du 25 mai 2018, seul le RGPD fait foi.**
- **Création d'un comité européen dédié à la protection des données.**

Qui est concerné ?

- Toute personne ou structure, exerçant une activité professionnelle / économique et «responsable du traitement de données ou sous-traitant».
- Toutes les entreprises européennes.
- Toutes les entreprises qui récoltent des données sur des personnes membres de pays de l'union européenne.

RGPD : objectifs et enjeux

Renforcer ma protection

Obligation de **réfléchir à la protection des données personnelles en amont de la conception d'un produit ou d'un service**.
En clair, dès que vous lancez un projet, vous devez prévoir la sécurité des données.

La donnée personnelle en bref…

AVANT LA RGPD

- Une donnée personnelle d'un utilisateur transite souvent entre plusieurs entreprises/prestataires (communication à des tiers, traitement, revente de données)
- Utilisateur -> pas informé des manipulations sur ses données ou du niveau de sécurité
- Aucun moyen pour l'utilisateur de savoir si ses données sont traitées de quelque façon que ce soit

APRES LA RGPD

- Désormais -> obligation d'avoir le consentement de l'utilisateur pour utiliser ses données + information sur demande du traitement effectué sur les données.
- Si refus -> aucune manipulation possible
- Possibilité de demander la suppression de ses données, s'il y a eu atteinte à la vie privée, notion de droit à l'oubli/effacement.

Quels services manipulent des données à caractère personnel ?

- **Marketing /commercial**
via la personnalisation des produits et des services, analyse comportementale, gestion de la relation client…

- **RH – Compta**
via le recrutement, gestion de carrière, suivi des compétences, suivi du temps de travail, paie…

- **R & D**
Développement de nouveaux
services et produits

- **Service informatique**
Maintenance des logiciels, exports de données, entrées/sorties, sécurité…

Exemples de donnée à caractère personnel

SERVICE MARKETING - COMMERCIAL

- Mail
- Adresse
- N° Téléphone
- Propriétaire – locataire
  Nbre enfants
  Anniversaires enfants…
  Poste occupé

SERVICE COMPTABILITÉ / RH

- Information des Salariés
- Information Bancaire
- Finance de l'Entreprise
- CV – Photo – Enregistrement video
- Dossier médical, n° de SS
- Données bio-métriques
- Notes de frais

SERVICE INFORMATIQUE

- Données d'inscription
  - Autre...
  - Anniversaire
  - Identifiant - Mot de passe
  - Nom, prénom
  - Email
  - Adresse (pour les e-commerces)

Exemples de données sensibles

Données sur les mineurs

Le règlement fixe à 16 ans l'âge auquel le mineur peut consentir aux finalités du traitement sans l'autorisation du titulaire de la responsabilité parentale. En revanche, pour les enfants âgés de 13 à 16 ans, le représentant légal de l'enfant doit donner ou autoriser le consentement pour que le traitement soit licite

Données médicales

Données bancaires – financières (cas des experts comptables)

En bref, quelles sont mes obligations ?

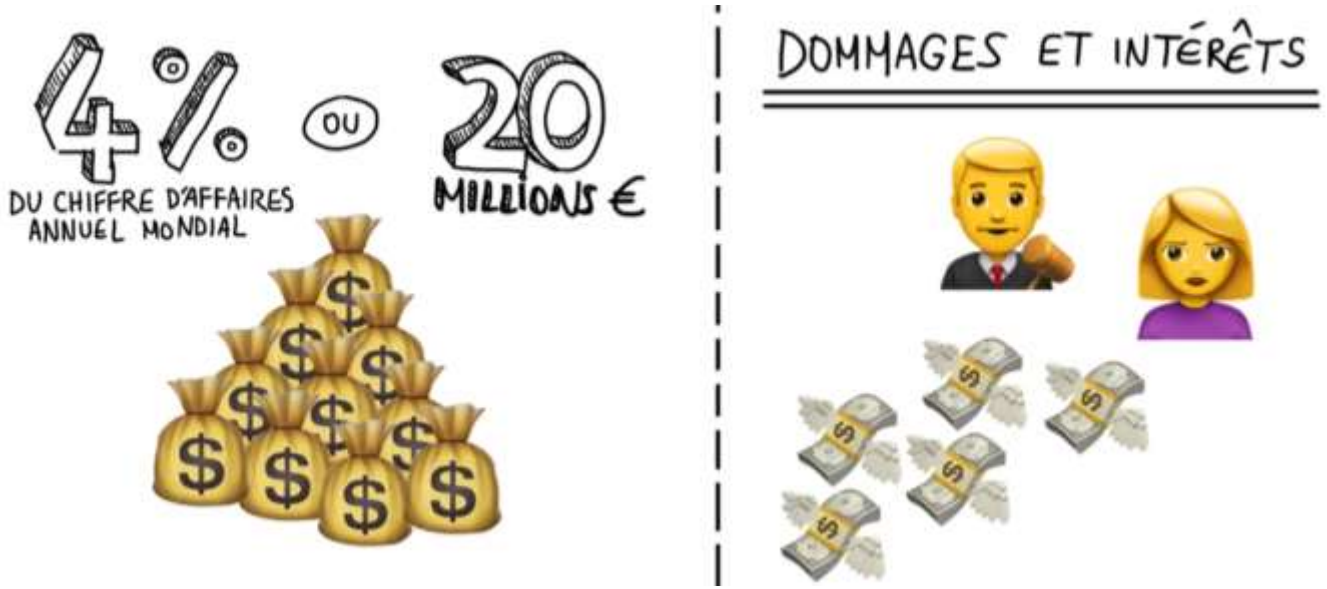
QUI EST PROTEGE : Toute information concernant ***« une personne physique identifiée ou identifiable » :*** salariés, candidats à un emploi, avocat, consultant, clients, prospects….

QUELLES DONNEES *:* toute information qui permet d'identifier une personne de manière directe ou indirecte : nom et prénoms, IBAN, téléphone, n° SS, dossier médical, image (enregistrement caméra, photos salariés), adresse mail, identifiant informatique, mot de passe, adresse IP…

QUOI FAIRE : Mettre en œuvre des mesures techniques et organisationnelles pour s'assurer de la conformité des traitements, de la sécurité autour des données et pouvoir le démontrer.

Quelles sont les sanctions encourues ?

- Un simple avertissement si c'est la première fois ou que la faute est non-intentionnelle.
- Une amende allant jusqu'à 10 000 000€ ou 2% du chiffre d'affaire annuel.
- Si le chiffre d'affaires de l'entreprise est de plus de 500 millions d'euros, la sanction peut être une amende allant jusqu'à 20 000 000€ ou 4% du chiffre d'affaire annuel (le montant le plus élevé peut être retenu).



RGPD

Les points essentiels de la loi

Principe	Explications	Exemple
Principe de minimisation	La collecte des données doit se cantonner au strict nécessaire.	un vendeur de produits cosmétiques n'a pas à savoir si son client est un amateur de séries télévisées.
Consentement	- Le règlement impose de rendre plus clair le consentement au traitement des données, par exemple au moyen d'une déclaration écrite ou par voie électronique. L'accord doit être « libre, spécifique, éclairé et univoque ». « Il ne saurait y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité, précise le règlement. […] - Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles. - Le consentement est le fondement au traitement des données. L'entreprise doit dans la mesure du possible intégrer la protection de la vie privée dès la conception du logiciel ou du service et mettre en place les outils adéquats pour préserver la liberté de choix de l'utilisateur.	Case à cocher pour recevoir les emails commerciaux, Case distincte pour les emais des partenaires Possibilité de cocher ou décocher la géolocalisation dans un smartphone…
Preuve du consentement	Lorsque le traitement est fondé sur le consentement de la personne concernée, le responsable du traitement doit être capable de prouver ce consentement.	Preuve numérique ou écrite du consentement.

Principe	Explications	Exemple
Mise en place d'outils	**Les outils de collecte ou gestion interne** de l'entreprise (CRM, logiciels, site) doivent permettre à l'utilisateur d'exercer son droit d'accès aux données, son droit de les rectifier, son droit de s'opposer à certains types de traitements	Mon logiciel qui gère mon fichier client (devis / facture) doit comporter des cases concernant le consentement.
Auto-responsabilisation	**Il appartient à l'entreprise** de prendre toutes les mesures nécessaires pour remplir ses obligations de protection des données, et être capable de le démontrer à tout moment. À cet effet, elle devra tenir un registre recensant les catégories de données traitées, les finalités du traitement, les pays où elles sont transférées, la durée de conservation, etc. **Les entreprises qui, notamment, traitent des données à grande échelle**, devront désigner un responsable délégué à la protection des données (DPO) dédié au contrôle de la conformité au GDPR (entreprise de plus de 250 collaborateurs). Conseillé pour toutes les entreprises	Registre des données + responsable désigné des données
Sécurité par défaut	L'entreprise doit prendre les mesures nécessaires pour **sécuriser les données**, notamment par le chiffrement ou la « pseudonymisation ». Elle doit aussi mettre en place des outils de détection de failles de sécurité. Elle doit être en mesure de prouver à n'importe quel moment, que les données à caractère personnel qu'elle détient, sont protégées et inexploitables en cas de vol.	Audit de mes outils et prestataires Audit de ma sécurité interne : cartographie du circuit de mes données et détection faille. Scénario de crise à prévoir.

Principe	Explications	Exemple
Droit à l'oubli numérique	**Durée de conservation** des données **Droit à l'effacement des données**, droit au déréférencement d'une information ou d'un lien par un moteur de recherche. **La personne peut s'adresser directement au responsable de traitement** dans le cas, par exemple, où l'entreprise a conservé ses données plus longtemps que nécessaire au vu des finalités annoncées.	**Relation client :** Adresse de contact où s'adresser en cas de demande d'effacement des données + processus d'effacement. Contrôle de la durée de conservation des données. **Ressources humaines :** Process interne pour les salariés d'avoir accès à leurs données et de pouvoir exercer leur droit d'opposition.
Réparation des dommages	**En cas de vol de données,** l'autorité doit être prévenue dans un délai maximal de 72 H. Les associations dédiées à la protection des données pourront introduire des recours collectifs. L'objectif est de faire cesser le dommage causé par la violation du règlement.	

Le délégué à la protection des données

Cette désignation est **obligatoire** en 2018, si :

- Vous êtes un organisme public.

- Vous êtes une entreprise dont l'activité de base vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Même si votre organisme/entreprise n'est pas formellement dans l'obligation de désigner un délégué à la protection des données, il est fortement recommandé d'en désigner un.

Rôle du délégué

Il est principalement chargé :

- **d'informer et de conseiller** les responsables de traitement ainsi que leurs employés
- **de contrôler le respect du règlement** et du droit national pour la protection des données
- **de conseiller l'organisme** sur la réalisation d'études d'impact et d'en vérifier l'exécution
- **de coopérer avec l'autorité de contrôle** et d'être le point de contact de celle-ci

Il doit également :

- **s'informer** sur le contenu des nouvelles obligations
- **sensibiliser** les décideurs sur l'impact de ces nouvelles règles
- **réaliser l'inventaire** des traitements de données de votre organisme
- **concevoir** des actions de sensibilisation
- **piloter** la conformité en continu.

RGPD et RH

UN AUDIT POUR :

- Quelles données à caractère personnel sont récoltées ?
- Le traitement est-il licite ? : Quelle base légale ? Consentement ?
- Quelle durée de conservation ?
- Et les sous-traitants ? (paye, SIRH….)
- Quels niveaux de sécurité ?
- Quelles améliorations apporter ?
- Les personnes peuvent-elles exercer leurs droits ?

POUVOIR PROUVER SA CONFORMITE

- Documenter et mettre en place le registre des traitements
- Tenir à jour le registre des traitements tels que ceux pour le recrutement, paie, registre du personnel, suivis des congés, BDES, entretiens individuels,…
- Pour chaque traitement : finalités, description, interlocuteurs, mesures de sécurité techniques et organisationnelles, quelles données à caractère personnel, licéité, destinataires du traitement, niveau de sécurité requis

LES DROITS DES PERSONNES CONCERNEES

- **Droit d'être informées** sur le fondement légal du traitement (ex : contrat de travail, loi,…) : établir la paye, transmettre les informations à l'URSSAF
- Le **consentement** : déclaration expresse
- **Droit à l'information** : coordonnées du responsable du traitement et finalités du traitement
- **Droit d'accès** : destinataires, durée de conservation, droit de rectification….
- **Droit à l'oubli** : droit de demander l'effacement de ses données personnelles
- **Droit à la limitation** du traitement : conserver sans utiliser
- **Droit à la portabilité** : droit de récupérer ses données, droit de les transférer

COMMENT SE METTRE EN CONFORMITE

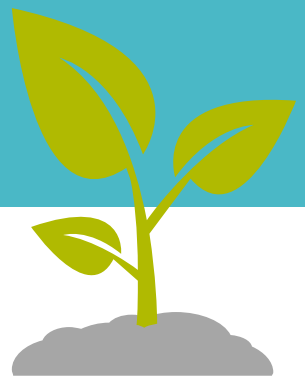
1 - **DRESSER UN ETAT DES LIEUX**

- Désigner un responsable, voire un délégué à la protection des données
- Auditer tous les traitements et les analyser

2 - **ELABORER UN PLAN D'ACTION ET CORRIGER LES NON-CONFORMITÉS**

3 –**ACTUALISER LE REGISTRE DE TRAITEMENT**

RGPD et **Marketing**

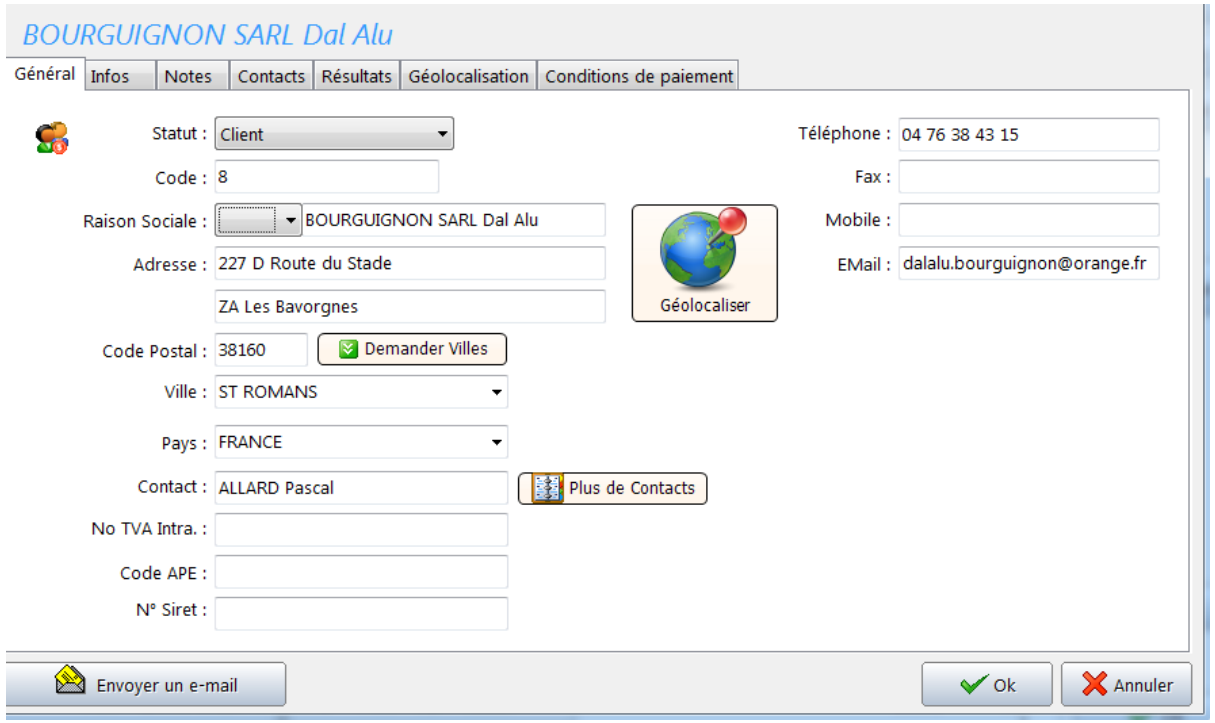


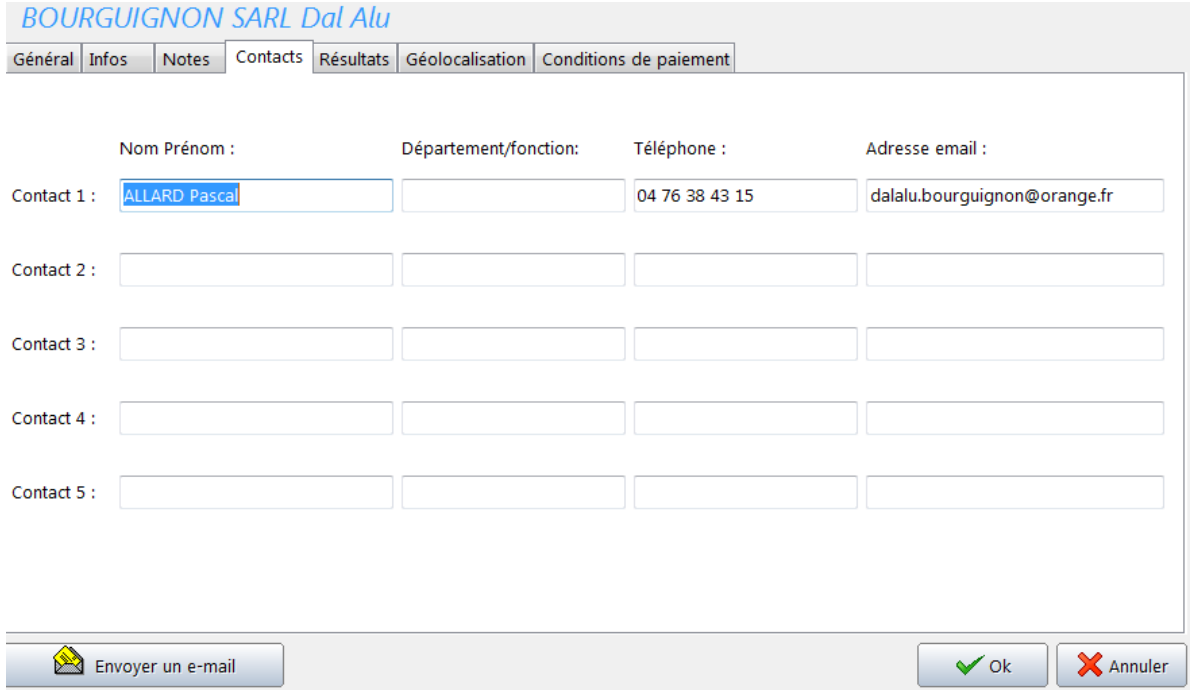
IMPORTANT

La RGPD s'adresse aussi bien à vos cibles BtoC que BtoB.

MON LOGICIEL EST-IL CONFORME ?

- Consentement ? Sécurité ? Droit à l'oubli ? Durée de stockage ?
- Abonnement ? Désabonnement ?





MES FORMULAIRES SONT-ILS CONFORMES ?

Nous rencontrer ?
250 chemin de Seillères
38160 Chatte

Nous envoyer un mail ?
contact@boostacom.fr

Nous téléphoner ?
06 26 94 14 19

Votre nom : *

Votre e-mail : *

Votre téléphone : *

Message : *

Envoyer

Laissez-nous votre message

Pour une demande de renseignements sur nos prestations, pour la rédaction d'un devis, ou pour une demande de rendez-vous, n'hésitez pas à nous contacter et nous vous répondrons dans les plus brefs délais !

Nous retrouver sur les réseaux sociaux:

PENSER MES EMAILINGS AUTREMENT

- Objectif : mettre fin également à l'e-mailing de masse envoyé à des contacts qui ne l'ont pas réellement désiré.

- Désormais, **le consentement doit être express et explicite** et là encore, **la finalité clairement stipulée ainsi que les destinataires**, si ces données personnelles devaient être partagées. **La personne concernée doit pouvoir accéder à ces données, les modifier si elles le souhaitent, les supprimer et interdire leur diffusion**.

- Les données personnelles que vous aurez ainsi recueillies ne peuvent être conservées que pour une **durée maximale de 3 ans**, et utilisées uniquement pour leur finalité de traitement.

- La preuve du consentement des destinataires de vos e-mails reste **à votre charge**, vous devrez donc en garder la trace, avec **la provenance et la date de création**.

OPTIMISER SES PROCESS ET SON IMAGE ?

- Documenter en interne les processus de récolte, de traitement des données personnelles, en levant d'éventuelles zones d'ombre.
- Bien (re)définir les finalités, les durées de conservation, qui en interne et en externe a accès aux données.
- Trier et mettre à jour les bases de données existantes en repérant les doublons et les données obsolètes, permettant ainsi de valoriser les données existantes.
- Adopter de bonnes pratiques d'information et de relation avec les prospects et clients (transparence sur les finalités, exercice des droits de communication, rectification, suppression, oubli, exportation).
- Améliorer et renforcer son image de marque.

RGPD : Par où commencer ?

Se poser les bonnes questions

Qui ?

Inscrire nom et coordonnées du responsable du traitement

Identifiez les responsables opérationnels traitant les données au sein de votre organisme

Où ?

Déterminez le lieu où les données sont hébergées.

Indiquez dans quels pays les données sont éventuellement transférées.

Quoi ?

Identifiez les catégories de données traitées

Identifiez les données à risques (par exemple, les données relatives à la santé ou les infractions)

Jusqu'à quand ?

Indiquez, pour chaque catégorie de données, combien de temps vous les conservez.

Pourquoi ?

Indiquez la ou les finalités pour lesquelles vous collectez ou traitez ces données

Comment ?

Quels outils conservent les données ?

Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données ?

Mettre en place la bonne organisation

1- IDENTIFIER LES TRAITEMENTS DE DONNÉES PERSONNELLES afin de créer un registre ;

2- PRIORISER LES ACTIONS À MENER pour vous conformer de manière logique et rapide ;

3- GÉRER LES RISQUES en faisant une analyse d'impact sur la protection des données (PIA) ;

4- ORGANISER LES PROCESSUS INTERNES qui garantissent la protection des données à tout moment ;

5- DOCUMENTER LA CONFORMITÉ et l'actualiser régulièrement pour assurer une protection en continu.

FRANÇOISE SILVAN
AVOCAT MEDIATEUR

BOOSTACOM
communication · digital · formation web

Merci de votre attention !
Des questions ?

Document téléchargeable sur www.boostacom.fr