Entr'actifs

RGPD : êtes-vous prêt ?

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

Sommaire

Contexte du RGPD

3

A l'ère du big data, nécessité de réglementer

- **Encadrer une pratique qui est devenue courante dans les usages : le stockage de données personnelles**
- **Mettre tous les pays européens au même niveau,** avec une réglementation européenne commune

4

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

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

5

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.

6

RGPD : objectifs et enjeux

Renforcer la protection
. Droits des citoyens renforcés

Réfléchir à la protection et à l'utilisation des données personnelles manipulées.
. Avoir un niveau de sécurité adapté au risque
. Conformité en continue (l'entreprise & ses sous-traitants ou partenaires)

7

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.

8

Exemples de donnée à caractère personnel

SERVICE MARKETING - COMMERCIAL

- Nom et prénom
- Mail
- Adresse
- N° Téléphone
- Propriétaire – locataire Revenus
- Nbre enfants Anniversaires enfants…
- Poste occupé

SERVICE COMPTABILITÉ / RH

- Information dossiers des Salariés, stagiaires…
- Information Bancaire
- CV – Photo
- Enregistrement caméra video - Pointage
- Notes de frais
- Dossier médical, n° de SS
- Données bio-métriques
- Compta de l'Entreprise : factures, devis

SERVICE INFORMATIQUE

- Données d'inscription
  - Identifiant - Mot de passe
  - Adresse IP
  - Liste et dates achats
  - Nom, prénom
  - Email
  - Adresse (pour les e-commerces)
- Gérer la sécurité des données (détection malveillance, chiffrage, accés…)

BOOSTACOM

9

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)

10

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…

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

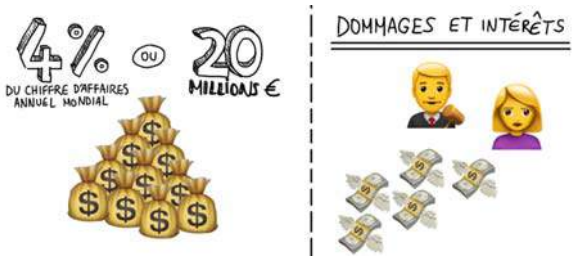
- **RH – Compta**
via le recrutement, gestion de carrière, suivi des compétences, suivi du temps de travail, paie…

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

11

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).



Comment vont se faire les contrôles ? Le risque d'être contrôlé est-il important ?

12

RGPD
Les points essentiels de la loi

Françoise S. peut vous en dire plus…

13

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.

14

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.

15

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 suppression 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 : nécessité Informer** rapidement la CNIL et les personnes concernées 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.	Prévoir un scénario de crise

16

RGPD et RH

Françoise S. peut vous en dire plus…

17

Faire un audit sur les données RH

- 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 ?

18

Exemple : le recrutement

Les membres d'un service RH devront s'assurer que cette loi est appliquée pour l'ensemble des salariés mais aussi pour les candidats à un poste. En effet, il va falloir obtenir l'approbation de celui-ci afin de pouvoir stocker les différentes données qui peuvent être demandées.

Il va falloir :

- Lui indiquer les coordonnées du délégué à la protection des données désigné dans l'entreprise,
- lui dire qu'il existe des organismes qui peuvent l'aider en cas de mauvaise application de la loi
- et si les données n'ont pas été récupérées auprès de la personne elle même, il faut mentionner qu'elles sont issues de source publique ou non.

19

Désigner un 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.

20

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.

21

Pouvoir prouver sa conformité

- **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

22

RGPD et Marketing

Cécile T. peut vous en dire plus…

23

IMPORTANT

Le RGPD concerne aussi bien vos clients BtoC que BtoB.

24

Sensibiliser l'équipe commerciale

- Il est important que les services commerciaux soient sensibilisés aux obligations qui s'imposent à eux. **Notamment dans le cas de collecte directe** (art.13 du RGPD).
- Les commerciaux devront se poser un certain nombre de questions afin de s'assurer d'être conforme avec les droits des personnes et les obligations des entreprises.
- D'après l'article 13, le commercial devra fournir un certain nombre d'informations lors de la collecte de données personnelles à la personne concernée (quel usage des données) et il devra garder une preuve du consentement + possibilité de rectifier ou supprimer la donnée par le prospect.

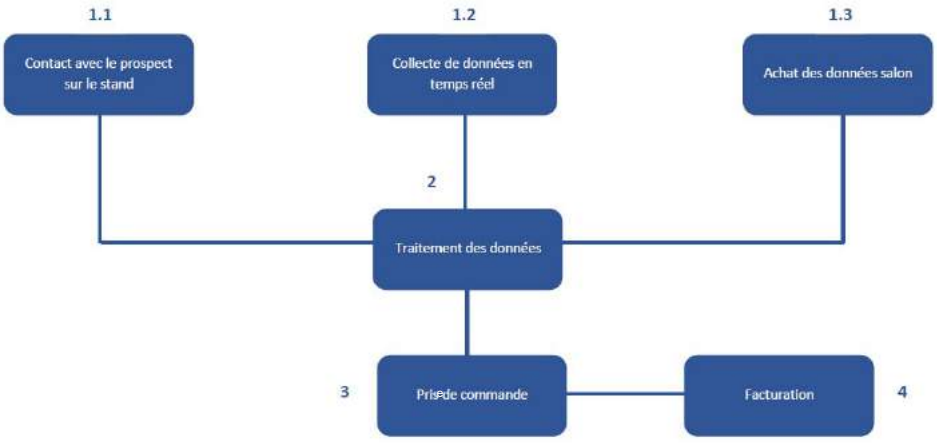
Exemple : fiche contact de salon – formulaire de devis – commerces / caisses enregistreuses (carte fidélité)

Mettre dans les Conditions Générales de Vente « L'entreprise met tout en œuvre pour garantir la protection de vos données, conformément aux directives du RGPD »

25

Ex. : je vais en salon commercial…

Le chemin des données



26

Penser ses emailings autrement

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

- Il faut obtenir le consentement préalable de l'utilisateur, de manière claire et explicite, et lui permettre de revenir sur cette décision facilement, afin de pouvoir exploiter son adresse e-mail dans un but marketing ou commercial.

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

27

La mise en conformité a déjà commencé…

28

En profiter pour optimiser son image et ses process ?

La RGPD, ce peut être l'occasion de …

- **Mieux s'organiser, mieux travailler avec des outils plus performants**
- **Trier et mettre à jour les bases de données** existantes en repérant les doublons et les données obsolètes
- **Adopter de bonnes pratiques d'information et de relation clients** : transparence sur les finalités, respect des droits de mes clients / prospects.
- **Améliorer et renforcer son image de marque** : le fait de respecter le RGPD et de le dire sur tous ses supports de communication, devient une force et un argument suscitant la confiance, par rapport à des concurrents qui ne le font pas.
- **Obtenir de marchés** grâce à sa conformité, quand les concurrents ne le sont pas encore

29

RGPD et web

Thomas L. peut vous en dire plus…

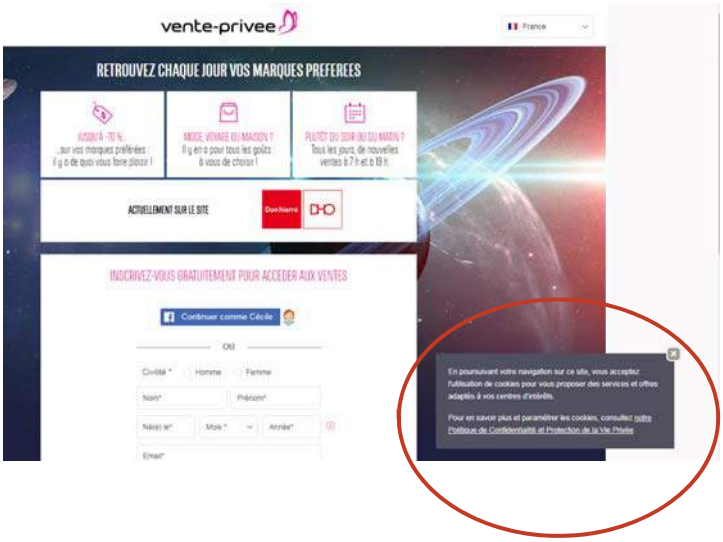
30

MON SITE EST-IL CONFORME ?

Mise à jour des CMS (plateforme technique de votre site) en cours
Seront à retravailler : Formulaires de contacts, Mentions Légales, CGV,

31

E-COMMERCE & GESTION DES COOKIES



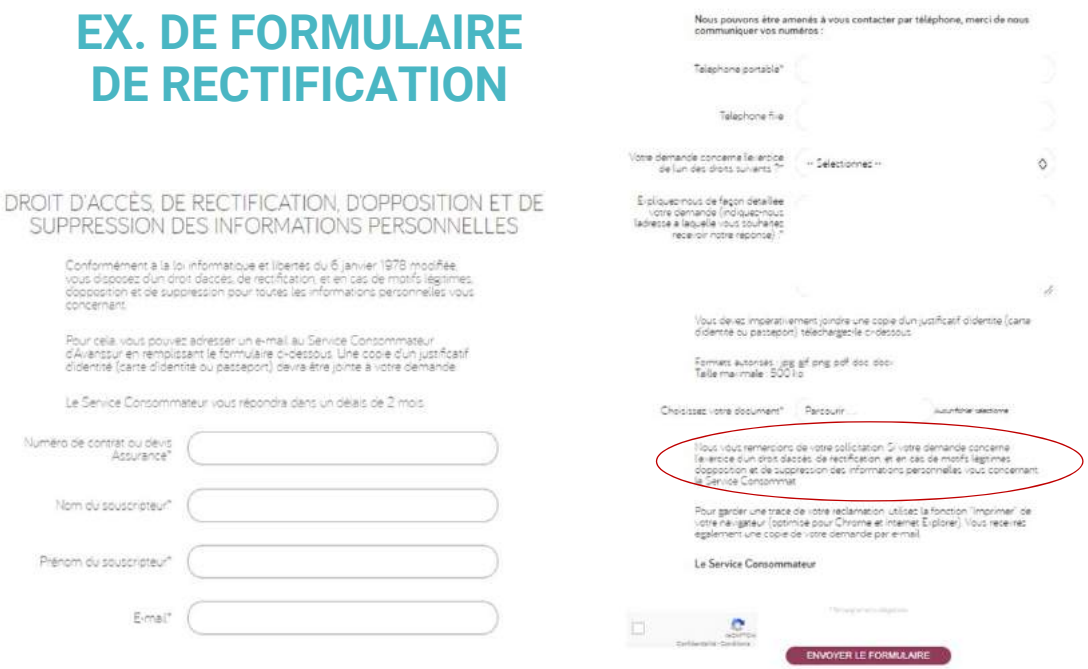
Cela signifie que le popup actuellement en place sur de nombreux sites web, demandant aux internautes, de façon vague, d'accepter l'utilisation des cookies pendant sa navigation, **devra être**

- **En place pour tous les sites, mêmes les site vitrines**
- **plus explicite qu'actuellement**. Il devra dire précisément quels seront les usages résultant de cette collecte de données.

Mais il faudra également donner à l'internaute le pouvoir de révoquer cette autorisation à tout moment (créer un formulaire de rectification).

32

EX. DE FORMULAIRE DE RECTIFICATION



DROIT D'ACCÈS, DE RECTIFICATION, D'OPPOSITION ET DE SUPPRESSION DES INFORMATIONS PERSONNELLES

Conformément à la loi informatique et libertés du 6 janvier 1978 modifiée, vous disposez d'un droit d'accès, de rectification, et en cas de motifs légitimes, d'opposition et de suppression pour toutes les informations personnelles vous concernant.

Pour cela, vous pouvez adresser un e-mail au Service Consommateur d'Avanssur en remplissant le formulaire ci-dessous. Une copie d'un justificatif d'identité (carte d'identité ou passeport) devra être jointe à votre demande.

Le Service Consommateur vous répondra dans un délais de 2 mois.

Numéro de contrat ou devis Assurance*

Nom du souscripteur*

Prénom du souscripteur*

E-mail*

Nous pouvons être amenés à vous contacter par téléphone, merci de nous communiquer vos numéros :

Téléphone portable*

Téléphone fixe

Votre demande concerne l'exercice de l'un des droits suivants ?*

-- Sélectionnez --

Expliquez-nous de façon détaillée votre demande (indiquez-nous l'adresse à laquelle vous souhaitez recevoir notre réponse) *

Vous devez impérativement joindre une copie d'un justificatif d'identité (carte d'identité ou passeport) téléchargez-le ci-dessous.

Formats autorisés : .jpg .gif .png .pdf .doc .docx
Taille maximale : 500 Ko

Choisissez votre document*

Parcourir...

Aucun fichier sélectionné

Nous vous remercions de votre sollicitation. Si votre demande concerne l'exercice d'un droit d'accès, de rectification et en cas de motifs légitimes d'opposition et de suppression des informations personnelles vous concernant, le Service Consommat

Pour garder une trace de votre réclamation, utilisez la fonction "Imprimer" de votre navigateur (optimisé pour Chrome et Internet Explorer). Vous recevrez également une copie de votre demande par e-mail.

Le Service Consommateur

ENVOYER LE FORMULAIRE

33

RGPD et informatique / logiciel

Delphine C., Sébastien P., Sébastien G.. peuvent vous en dire plus…

34

Comment sont stockées et sauvegardées mes données

– Comment sont protégés les ordinateurs ? Mot de passe ?

- Sécurité accés wifi ? Sécurité téléphones mobiles ?
- Serveur ? Fichier de données avec mot de passe ?

Se poser les questions sur sa façon de travailler.

35

Mon logiciel devis/facture est-il conforme ?

Vous devrez vérifier que votre solution est en conformité avec le RGPD

– Votre “sous-traitant” ou prestataire logiciel devra prouver sa conformité à la nouvelle réglementation (en gardant une trace écrite de vos échanges sur le sujet) ;

– Il devra également garantir l’intégrité et la sécurité des données récoltées de manière continuelle, pour éviter tout cas de piratage ou de brèche informatique ; ex . imprimer le certificat du logiciel « sécurité anti-fraudes > dans la rubrique aide du logiciel)

– Il devra prouver la suppression des données si l’internaute en fait la demande (en gardant en historique la date d’ajout, la date de demande de suppression, et la preuve de la suppression effective des données).

36

RGPD : Par où commencer ?

37

En résumé..

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

QUELLES DONNEES ?
toute information qui permet d'identifier une personne de manière directe ou indirecte (plusieurs données ensemble qui peuvent amener à identifier)

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 (preuves).

38

Se poser les bonnes questions

Tout simplement répondre à ces questions dans un tableau excel

1. Quoi ?

Identifiez les catégories de données traitées

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

2. Pourquoi ?

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

3. Où ?

Déterminez le lieu où les données sont hébergées.

Indiquez dans quels pays les données sont éventuellement transférées.

4. Comment ?

Quels outils conservent les données ?

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

5. Qui ?

Inscrire nom et coordonnées du responsable du traitement

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

6. Jusqu'à quand ?

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

39

Check list de mise en action

1. **Désigner un pilote de la mise en conformité :** doit avoir de bonnes notions informatiques
2. **Cartographier le traitement des données : le tableau excel questions**identifier quelles données, quels usages, quelles personnes ou quels sous-traitants, quels outils, quel stockage… avec commentaire sur actions à mener pour chaque étape
3. **Prioriser les actions à mener :** pour vous mettre en conformité de manière logique et rapide
4. **Identifier et gérer les risques :** analyse d'impact (**minime – moyen – fort)** sur la protection des données
5. **Réorganiser les process internes :** pour garantir la protection des données à tout moment (qui manipule, comment, relations sous-traitants…)
6. **Bien documenter sa conformité :** document à écrire (cartographie, preuves de conformité, process, scénario de crise) et à actualiser
7. **En profiter pour communiquer sur sa conformité** et booster son image ! ;-)

40

FRANÇOISE SILVAN
AVOCAT MÉDIATEUR

BOOSTACOM
communication · digital · formation web

licom DÉVELOPPEMENT

Merci de votre attention !
Des questions ?

Document téléchargeable sur www.boostacom.fr