Dune x Agence Somme Tourisme > GoSomme

Professionnels du tourisme : faire du RGPD un atout commercial

Atelier du 21 novembre 2023

Sommaire

Introduction sur la protection des données

- Qui est concerné par le RGPD ?
  - Cible
  - Champ d'application territorial
  - Champ d'application matériel
- Pourquoi mettre en avant sa conformité au RGPD

I. Ce qu'il faut retenir sur le RGPD et les données personnelles

- Rappel sur les grands principes
- Quelles obligations vis-à-vis des prospects/clients
- Quelles obligations vis-à-vis des partenaires
- Focus sur la prospection commerciale

II. Bonnes pratiques dans le secteur du tourisme

- Site internet & cookies
- Faut-il désigner un DPO ?
- Réagir à une demande d'accès ou d'effacement
- Astuces & boite à outils
- Actualités dans le secteur du tourisme
- A quel coût se mettre en conformité au RGPD

III. Partage d'expérience / questions

INTRODUCTION

Principaux textes sur les données personnelles

RGPD
(27 avril 2016)

- Applicable depuis le 25 mai 2018
- Applicable dans tous les Etats membres de l'Union Européenne

Loi Informatique et Libertés
(modifiée le 20 juin 2018 et par l'ordonnance du 13 décembre 2018 applicable en juin 2019)

- Nouvelles dispositions applicables depuis le 21 juin 2018 sous réserve de nouveaux changements à venir au plus tard au 1er juin 2019
- Complétée par la doctrine de la CNIL et les décisions de justice

Sanctions communes

Lexique du RGPD

Notions de base

Données personnelles

Données sensibles

Traitement

Finalité d'un traitement

Base légale

DPO

CNIL

Lexique du RGPD

Notions avancées

Opt-in

Opt-out

Cookies

Accountability

Registre des activités de traitement

Analyse d'impact

Violation de données

Traitements de données personnelles

Collecte
(ex. formulaire)

Exploitation
(ex. analyse)

Suppression

Utilisation
(ex. envoi emails)

Diffusion
(ex. transfert)

Consultation

Enregistrement
(ex. sauvegarde)

Interconnexion
(ex. mettre en relation des fichiers)

Structuration
(ex. classement)

Modification
(ex. rectification)

Qui est concerné par le RGPD ?

👉 Champ d'application matériel

- **Organisation publique**
- **Organisation privée**
- Exclusions: traitement dans le cadre d'une activité strictement personnelle ou domestique

👉 Champ d'application territorial

- Organisation établie sur le territoire de l'Union Européenne
- Organisation non européenne ciblant directement des résidents européens par ses produits ou ses services
- Organisation opérant un suivi du comportement des résidents européens

Pourquoi mettre en avant sa conformité au RGPD

Plusieurs raisons variées :

- Obligation légale (mentions d'information)
- Partie intégrante de la responsabilité sociale des entreprises
- Meilleure connaissance des données stockées
- Optimisation de l'utilisation des données
- Atout auprès de ses clients et de ses partenaires
- Gage de sérieux auprès des prospects et du public
- Due diligence sur le RGPD dans les opérations de fusions-acquisitions

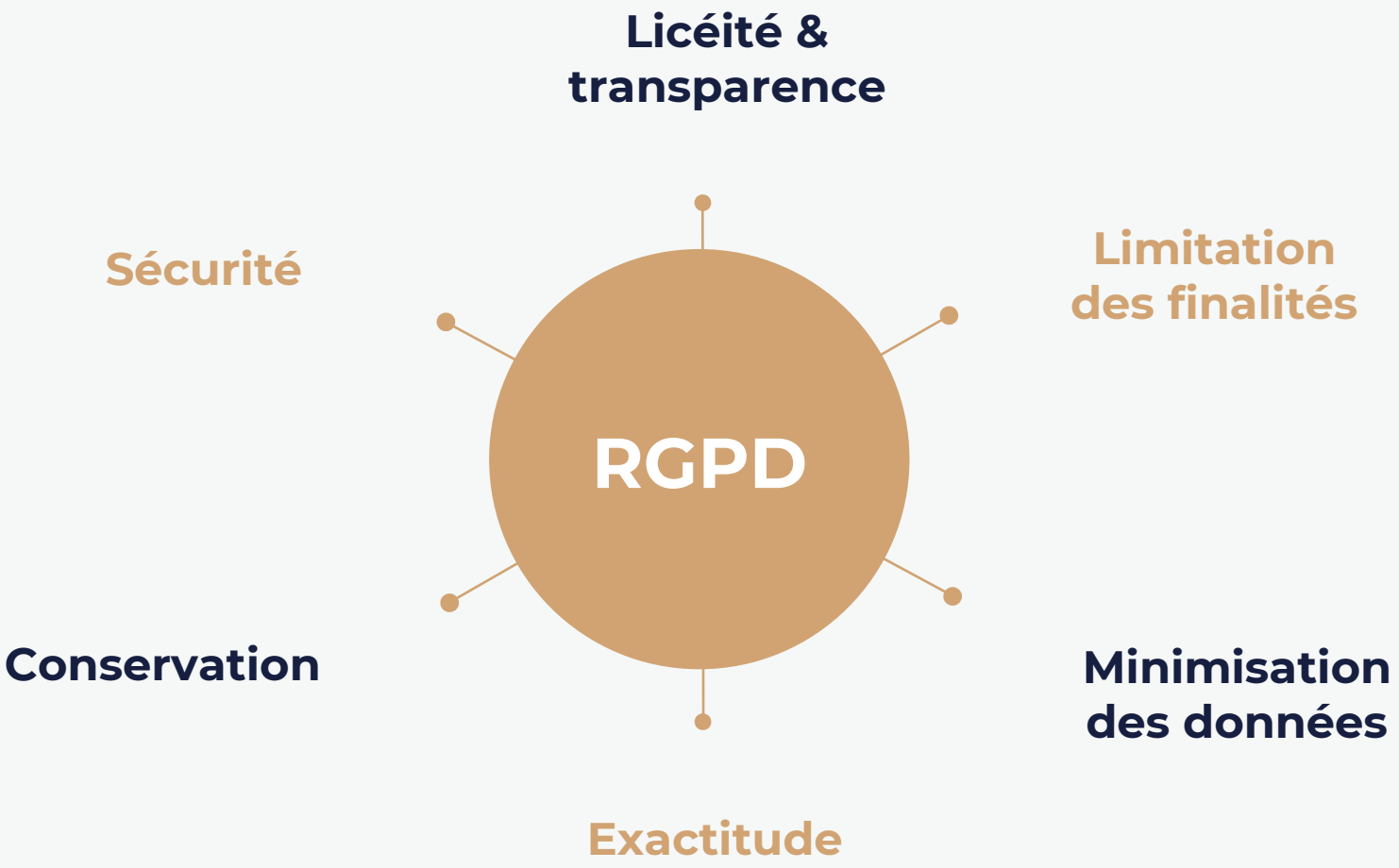
1

CE QU'IL FAUT RETENIR SUR LE RGPD ET LES DONNÉES PERSONNELLES

Rappel sur les grands principes

LORS DE LA MISE EN PLACE D'UN TRAITEMENT, IL FAUT VEILLER AU RESPECT DES PRINCIPES DE :

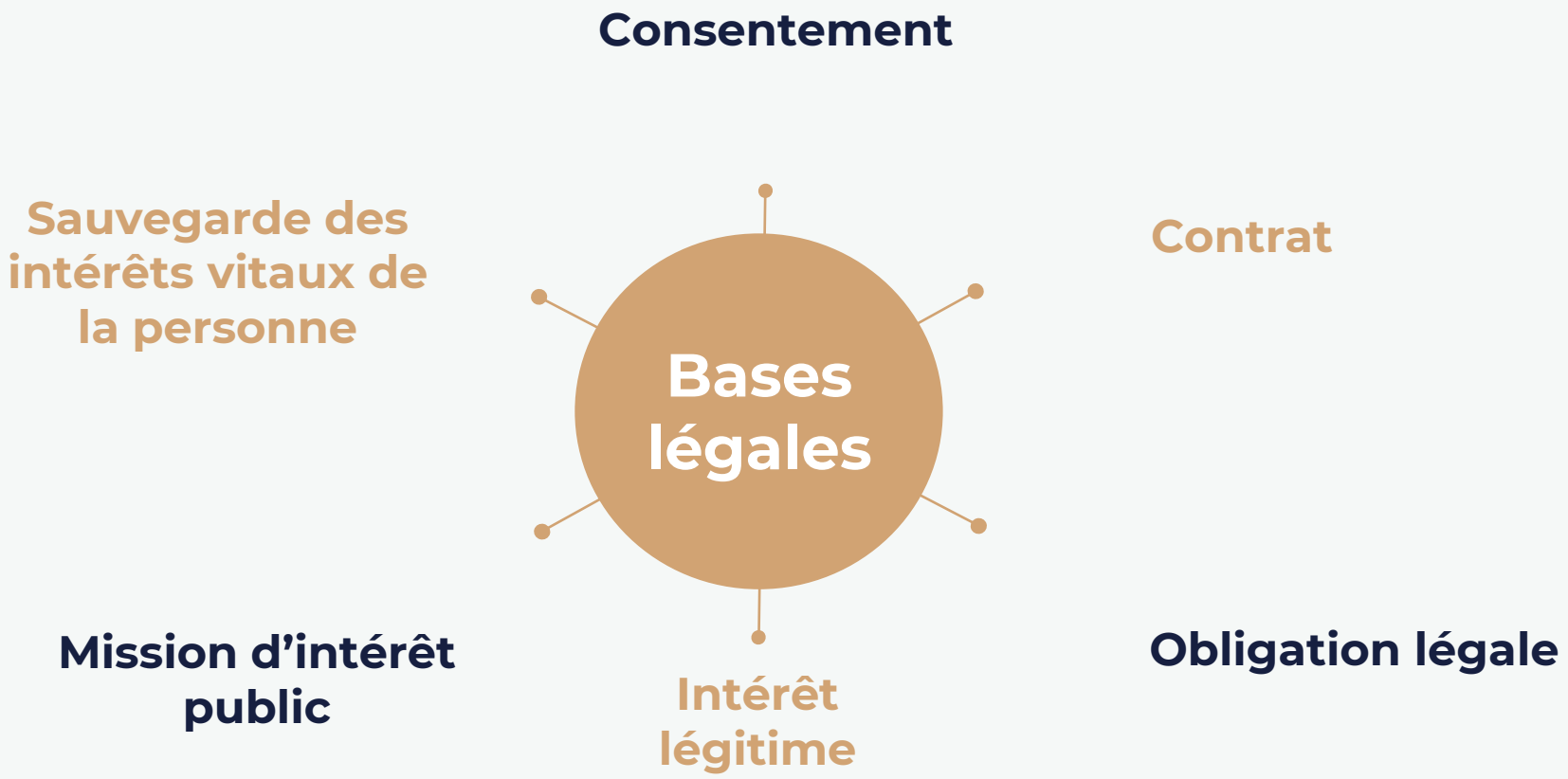
- ***Privacy by design***
- ***Privacy by default*** **: par défaut, les données sont traitées selon le plus haut niveau de confidentialité**



Bases légales pouvant fonder un traitement

La règlementation impose que tout traitement soit mis en œuvre sur une base légale dont la liste est définie par le RGPD.

Le responsable du traitement doit justifier de la base légale des traitements qu'il met en œuvre.



Acteurs d'un traitement

La règlementation distingue principalement trois catégories d'acteurs qui peuvent intervenir dans un traitement de données à caractère personnel.

RESPONSABLE DU TRAITEMENT

- Entité qui détermine **les moyens** et **finalités** du traitement.
- Il doit s'assurer que ses traitements respectent le RGPD et que les sous-traitants auxquels il fait appel respectent celui-ci.

RESPONSABLES CONJOINTS

- Entités qui déterminent **conjointement** les moyens et finalités du traitement.

Conséquences de la qualification :

- **Mise en place d'un contrat entre les co-responsables indiquant le rôle de chaque co-responsable dans le traitement**
- **Information des personnes de cette co-responsabilité**

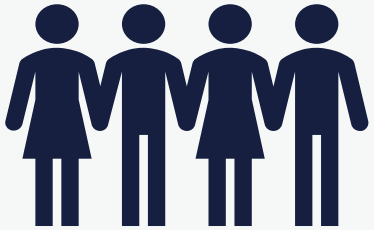
SOUS-TRAITANTS

- Entité qui traite des données à caractère personnel pour le compte du responsable du traitement
- Le sous-traitant n'utilise pas les données pour son propre compte : il les utilise uniquement selon les instructions données par le responsable du traitement.

Conséquences de la qualification :

- **Mise en place d'un contrat avec clauses obligatoires du RGPD**
- **Création d'un registre des activités de traitement spécifique à la sous-traitance.**

Droits des personnes concernées sur leurs données



Personnes Concernées

Droit d'être informé(e) avant la collecte et en cours de traitements *NB : les informations à fournir sont listées aux articles 13 et 14 du RGPD*
Droit d'accès pour déterminer quelles données sont traitées
Droit de demander la rectification des données
Droit de demander l'effacement des données
Droit de demander une limitation du traitement (gel)
Droit de s'opposer au traitement
Droit à la portabilité des données dans un format structuré et lisible
Droit à l'intervention humaine face à un profilage ou à une décision automatisée
Droit d'introduire une réclamation auprès d'une autorité de contrôle, en France, la CNIL

Quelles obligations vis-à-vis des prospects/clients (BtoC)

1. Informer et respecter les droits

2. Sécuriser le traitement

3. Respecter des durées de conservation

4. Documenter

Quelles obligations vis-à-vis des partenaires (BtoB)

0. Choisir votre partenaire, déterminer votre rôle et celui du partenaire

1. Informer et respecter les droits

2. Sécuriser le traitement

3. Respecter des durées de conservation

4. Documenter

Focus sur la prospection commerciale

👉 Pas de définition de la prospection dans le RGPD

Prospection = envoi de tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services.

Code des Postes et des Communications Electroniques (« **CPCE** »)

Notion entendue et interprétée largement par la CNIL.

Règle = consentement libre, spécifique, éclairé et univoque de la personne (*opt-in)*

= base légale du traitement des données

Focus sur la prospection commerciale par email ou SMS

Pour la prospection par voie d'email ou de SMS : trois exceptions pour mettre en place un droit d'opposition (un *opt-out*) :

Exception 1

Cliente de l'entreprise

Prospection concerne des produits et services similaires à ceux qu'elle a achetés

(article L. 34-5 alinéa 4 du CPCE)

Exception 2

Communication non commerciale (par exemple, caritative ou politique)

(CNIL)

Exception 3

Destinataire = professionnel

Prospection est en rapport avec la profession de la personne démarchée.

(CNIL)

👉 Dans tous les cas, la personne concernée doit être informée, au moment de la collecte de ses données, que celles-ci seront utilisées à des fins de prospection.

2 BONNES PRATIQUES DANS LE SECTEUR DU TOURISME

Site internet & cookies

La simple poursuite de la navigation sur un site ne vaut plus consentement au dépôt de cookies.

Consentement préalable aux cookies et pour chaque finalité :

Le visiteur doit consentir aux finalités des Cookies (pas dans les conditions générales ou une politique de confidentialité).

Les informations devant être portées à la connaissance des visiteurs sont, à tout le moins l'identité, du ou des responsables de traitement, la finalité des opérations de lecture ou écriture des données et l'existence du droit de retirer son consentement.

Exception au consentement préalable :

- Cookies ayant pour finalité exclusive de permettre ou faciliter la communication par voie électronique ; ou
- Cookies strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur, sous réserve que ce dernier soit informé de leur existence et de leur finalité.

👉 **Pour plus d'information**

Lignes directrices sur les Cookies du 17 septembre 2020 de la CNIL ainsi que des recommandations. La période d'adaptation pour se mettre en conformité avec ces lignes directrices et recommandations s'est achevée le 31 mars 2021.

Site internet & cookies : étude de cas

Désignation d'un DPO ou pas ?

Qu'est-ce qu'un DPO ?

- Personne chargée de mettre en œuvre la conformité au RGPD au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme
- Interlocuteur privilégié de la CNIL au sein de l'organisme
- Point de contact des personnes concernées par le traitement des données
- DPO interne (salarié) ou DPO externalisé (contrat de prestations de services)

Un DPO est-il obligatoire ?

- Traitements opérés par des autorités ou des organismes publics
- Organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle
- Organismes dont les activités de base les amènent à traiter à grande échelle des données sensibles ou relatives à des condamnations pénales et infractions

Désignation d’un DPO ou pas ?

- Mission d’information et de conseil auprès du responsable du traitement ou du sous-traitant ainsi que leurs employés
- Mission de contrôle de respect du RGPD et du droit national en matière de protection des données
- Mission de conseiller de l’organisme sur la réalisation d’une analyse d’impact relative à la protection des données et d’en vérifier l’exécution
- Mission de coopération avec la CNIL en étant le point de contact
- Mission de participation à la documentation. Exemple: la tenue du registre des traitements.

Soumis au secret professionnel ou à une obligation de confidentialité

Autonome et indépendant

Multi-tâches sous réserve de l’absence de conflits d’intérêts

Réagir à une demande d'accès ou d'effacement

👉 Lors de la réception d'une demande

1. Accuser réception de la demande en indiquant au requérant qu'il lui sera répondu sous un mois, sauf prolongation de deux mois supplémentaires
2. Vérifier l'identité au requérant pour s'assurer qu'il ne s'agit pas d'une demande frauduleuse.

Attention : il n'est pas possible de demander une photocopie de la carte d'identité (sauf en cas de doute raisonnable).

Si une copie de pièce d'identité a été demandée, la copie doit **impérativement** être supprimée une fois la vérification réalisée.

3. Qualifier le droit exercé (accès, rectification, suppression, portabilité, opposition, limitation ou retrait du consentement).
4. Vérifier si la demande du requérant est valide, c'est-à-dire si :
   - la demande ne rentre pas dans une hypothèse d'exception au droit exercé, listée dans le RGPD ;
   - la demande n'est pas abusive ; et
   - le requérant peut être identifié.

👉 Une fois l'identité du requérant vérifiée et le ou les droits exercés qualifiés : il convient d'identifier les personnes au sein de l'organisation qui pourront prendre en charge la demande.

👉 Ensuite, la demande devra être traitée.

👉 Si vous recevez beaucoup de demandes, il peut être utile de :

- tenir un registre des demandes d'exercice de droits reçues afin de suivre les délais pour répondre, les mesures prises pour répondre, et les personnes en charge de cette demande ;
- rédiger des réponses types, afin de faciliter la prise en charge des demandes ;
- créer une procédure de gestion des exercices de droits.

Les bonnes questions qu'il faut se poser et les bonnes pratiques

- Quoi? Pourquoi? Combien de temps ? Où ? Comment ? Toutes les données sont-elles utiles et nécessaires? Qui y a accès ?
- Quelle base juridique au traitement ? Quels destinataires des données et où sont-ils localisés ?
- Préparer un document d'information, clair et simple, informant les personnes concernées du traitement de leurs données et des réponses types pour répondre facilement à leurs exercices de droits
- Privilégier des solutions permettant un hébergement des données au sein de l'UE ou de pays disposant d'une législation équivalente
- Préparer une documentation pour les clients, permettant de démontrer que le RGPD est respecté et listant les mesures de sécurité appliquées
- Constituer la documentation de conformité et la regrouper au sein d'un même dossier, et permettre un accès simple à cette documentation

Exemple de roadmap pour mettre en conformité son entreprise

La frise chronologique ci-contre indique les principales étapes à mettre en œuvre au sein de son organisme pour préparer sa conformité au RGPD

Ressources utiles de la CNIL pour déterminer les actions à mettre en œuvre:
l'évaluation du niveau de maturité

1.
Cartographier

2.
Identifier les actions à réaliser

3.
Évaluer et gérer les risques

4.
Organiser les procédures internes

5.
Documenter la conformité

Bonnes pratiques : avoir le réflexe RGPD !

- Penser au RGPD dès la mise en place d'un nouveau service ou changement des modalités d'un service
- Continuellement améliorer sa conformité au RGPD

Astuces & boite à outils : mentions d'information sur le site de la CNIL

Version exhaustive :

Les informations recueillies sur ce formulaire sont enregistrées dans un fichier informatisé par **[identité et coordonnées du responsable de traitement]** pour **[finalités du traitement]**. La base légale du traitement est **[base légale du traitement]**.

Les données collectées seront communiquées aux seuls destinataires suivants : **[destinataires des données].**

Les données sont conservées pendant **[durée de conservation des données prévue par le responsable du traitement ou critères permettant de la déterminer]**.

Vous pouvez accéder aux données vous concernant, les rectifier, demander leur effacement ou exercer votre droit à la limitation du traitement de vos données. **(en fonction de la base légale du traitement, mentionner également : Vous pouvez retirer à tout moment votre consentement au traitement de vos données ; Vous pouvez également vous opposer au traitement de vos données ; Vous pouvez également exercer votre droit à la portabilité de vos données)**

Consultez le site cnil.fr pour plus d'informations sur vos droits.

Pour exercer ces droits ou pour toute question sur le traitement de vos données dans ce dispositif, vous pouvez contacter **(le cas échéant, notre délégué à la protection des données ou le service chargé de l'exercice de ces droits) : [adresse électronique, postale, coordonnées téléphoniques, etc.]**

Si vous estimez, après nous avoir contactés, que vos droits « Informatique et Libertés » ne sont pas respectés, vous pouvez adresser une réclamation à la CNIL.

Version courte :

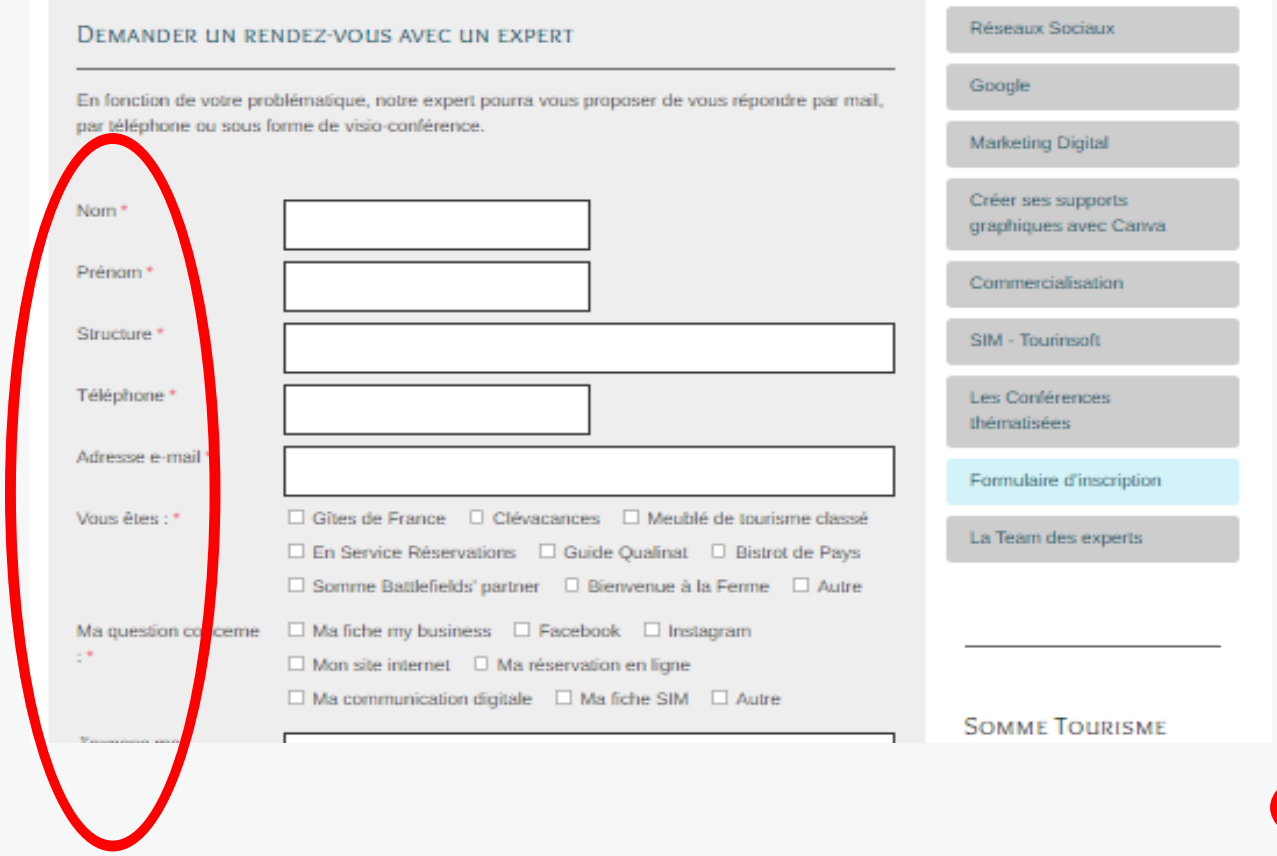
Abonnez-vous à la lettre d'information

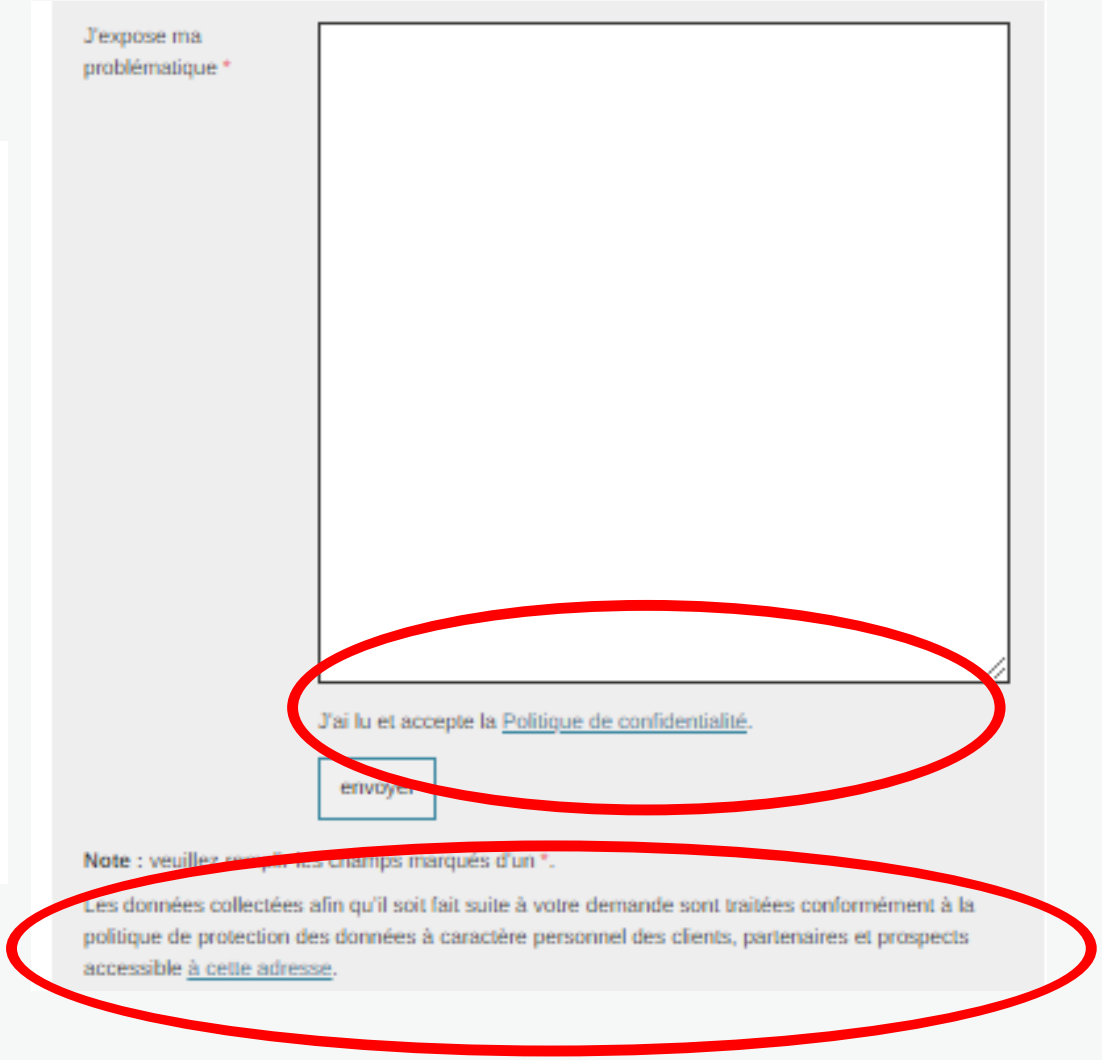
nom@exemple.fr

S'INSCRIRE À LA LETTRE D'INFORMATION

Votre adresse de messagerie est uniquement utilisée pour vous envoyer les lettres d'information de la CNIL. Vous pouvez à tout moment utiliser le lien de désabonnement intégré dans la newsletter. ***En savoir plus sur la gestion de vos données et vos droits***

Astuces & boite à outils : étude de cas de mentions d'informations





Astuces & boite à outils : exemple de registre

Description du traitement	
Nom du traitement	
N° / RÉF	ref-001
Date de création du traitement	
Mise à jour du traitement	

Acteurs	Nom	Adresse	Code Postal	Ville	Pays	Téléphone	Adresse mél
Responsable du traitement							
Délégué à la protection des données							
Société du DPO (si celui-ci est externe)							
Représentant							
Responsable(s) conjoint(s)							

Finalité(s) du traitement effectué	
Finalité principale	
Sous-finalité 1	
Sous-finalité 2	

Catégories de données personnelles concernées	Description	Durée de conservation
État civil, identité, données d'identification, images…		
Vie personnelle (habitudes de vie, situation familiale, etc.)		
Informations d'ordre économique et financier (revenus, situation		

Catégories de personnes concernées	Description	Précisions
Catégorie de personnes 1	Sélectionnez un élément dans cette liste déroulante	
Catégorie de personnes 2		

Destinataires	Type de destinataire	Précisions
Destinataire 1	Sélectionnez un élément dans cette liste déroulante	
Destinataire 2		

Mesures de sécurité	Type de mesure de sécurité	Précisions
Mesure de sécurité 1	Sélectionnez un élément dans cette liste déroulante ▶	
Mesure de sécurité 2		
Mesure de sécurité 3		

Transferts hors UE	Destinataire	Pays	Type de Garanties	Liens vers la documentation
Organisme destinataire 1		Sélectionnez un élément dans cette	Sélectionnez un élément dans cette liste déroulante ▶	
Organisme destinataire 2				

Astuces & boite à outils : désignation CNIL

Exemple : formulaire de désignation du DPO sur le site de la CNIL

CNIL.

> Vos démarches > Désigner un DPO

Désignation d'un délégué à la protection des données

4 étapes pour finaliser votre désignation

ORGANISME (1) — DÉLÉGUÉ (2) — COORDONNÉES PUBLIQUES (3) — RÉCAPITULATIF ET ENVOI (4)

Quelles obligations vis-à-vis de...

Organisme désignant le délégué

Tous les champs de ce formulaire sont obligatoires

IDENTIFICATION DE L'ORGANISME

Numéro SIREN

Vérifier

☐ Cochez cette case si votre organisme ne dispose pas de N° SIREN

Etape suivante

A quel coût se mettre en conformité au RGPD

€€€

- Coût de l'audit juridique : cartographie des flux, évaluation des points de conformité/ non-conformité et mesures de remédiation
- Coût de l'audit technique : évaluation du système d'information (mesures de sécurité, détection des failles)
- Coût d'un juriste en données personnelles / prestataire externe pouvant assurant le rôle de DPO
  - Répondre aux demandes internes et externes
  - Accompagner l'entreprise
  - Alerter l'entreprise
  - Tenir la documentation d'*accountability*
- Coût des opérationnels qui vont consacrer du temps pour la mise en conformité au RGPD
- Coût pour le développement informatique

Liens vers des sites internet utiles

CNIL	Accéder aux informations de la CNIL
Légifrance	Accéder aux textes légaux et aux décisions de justice
CEPD	Accéder aux informations du CEPD
Legalis	Consulter les décisions de justice en droit des données
Doctrine du Groupe Article 29	Consulter la documentation du Groupe Article 29
Dune	Notre site contenant un blog et des informations utiles

3 PARTAGE D’EXPÉRIENCE / QUESTIONS

Merci pour votre attention !

Les + Dune

Valoriser son entreprise & optimiser ses contrats

Notre ADN et nos offres

- Direction juridique externalisée réactive et autonome
- Cabinet pluridisciplinaire : notre équipe intervient en
  - Droit des nouvelles technologies et des données
  - Droit des affaires
  - Droit social
  - Propriété intellectuelle
- Notre organisation de travail
  - Fourniture de recommandations et conseils clairs et opérationnels
  - Défense de vos intérêts en cas de contentieux
  - Pionniers dans l'utilisation des technologies numériques
- Plus d'information sur nos offres RGPD 👉 ici

Les extras Dune

- Le Blog Dune pour être à jour des actualités juridiques
- Abonnement à notre newsletter
- Dune Collabs : (ré)écouter nos podcasts ou (re)voir nos webinars *(Bien documenter sa conformité RGPD ; Comment la crise sanitaire liée au Coronavirus a remis le RGPD sur le devant de la scène)*

DUNE

Contact et information

5, rue du Chevalier de Saint-George 75008 Paris

+33(0)1 85 65 03 23
dune.fr