Visioconférence

« Mise en règles RGPD* pour mon tiers-lieu »

*Règlement Général sur la Protection des Données

jeudi 16 février 2023

Nous avons souhaité aborder ce thème en visioconférence car nombre de tiers-lieux ignorent qu'ils sont concernés par le Règlement Général sur la Protection des Données, certains ne savent comment le mettre en œuvre ou encore le mettent en œuvre partiellement par ignorance.

Cette note vise à synthétiser les grands thèmes abordés durant la visioconférence par les intervenants mais également par les participant.e.s au travers des questions qu'ils ou elles ont pu poser.

Objectifs

- Sensibiliser à la RGPD
- Connaître la réglementation en vigueur
- Identifier les étapes de la mise en oeuvre

Partenaires - intervenants

- Virginie Giraud, formatrice juriste consultante – RGPD, protection des majeurs, législations secteurs social et médico-social.
  virginie.giraud@formation24.net - 06.83.03.44.77

Grands axes évoqué

C'est quoi la protection des données personnelles en France ?

La protection des données personnelles est le respect de droits que nous avons tous basé sur deux cadres légaux : la loi informatique et libertés d'une part, le RGPD d'autre part.

Quelques fondamentaux sur le cadre légal dans l'histoire en France
2 jurisprudences

L'affaire SAFARI. A l'origine de la loi informatique et libertés de 1978, SAFARI est un projet du gouvernement élaboré en 1973. Il s'agirait d'un méga fichier d'informations administratives pour toutes les administrations françaises afin de tout savoir sur les citoyens français. Ce projet a fait beaucoup de bruit, la presse s'est emparée de ce sujet.

Projet soutenu par la Région Nouvelle-Aquitaine et l'Union Européenne dans le cadre du « Programme Opérationnel FEDER / FSE 2014-2020 »

Pourquoi le nom de “SAFARI” ? C’est simplement le nom du système en question.

Ce projet soulève de nombreuses questions, entre autres : Que va-t-on mettre dans ce fichier ? Est-ce que le gouvernement va suivre de très près tous les citoyens ? Elles vont amener une réflexion sur la protection des données personnelles des citoyens français.

Cette réflexion a donné naissance à la loi informatique et libertés de 1978 qui a donné lieu à la mise en place de droits pour ceux dont on traite des données à caractère personnel, notamment :

- un droit d’information sur le traitement des données
- un droit d’accès aux données
- un droit de modification, suppression des données

La loi a créé des obligations envers les institutions et les professionnels qui traitent ces données à caractère personnel. Ainsi, le professionnel qui gère une association doit renseigner une déclaration préalable des données collectées qui est remise à la CNIL. De même, les professionnels qui traitent des données à caractère personnel vont également avoir des obligations d’information.

Elle a également créé la CNIL, autorité de référence dans la protection des données personnelles.

L’affaire CAMBRIDGE ANALYTICA. A l’origine de la création du RGPD en 2016, une “affaire”. Il s’agit d’une entreprise, CAMBRIDGE ANALYTICA, qui a siphonné des millions de données via facebook sur des utilisateurs sans rien dire à personne.

CAMBRIDGE ANALYTICA voit le jour en 2013. “Les données déterminent tout ce que nous faisons” est la baseline de cette entreprise qui construit des profils types et les influence dans certains événement notamment les élections présidentielles américaines. Un employé de cette entreprise avait bien indiqué qu’il s’était servi des données pour cibler les démons intérieurs des utilisateurs. Cette entreprise a été accusée d’avoir influencé de nombreux électeurs américains mais également anglais sur le Brexit d’où une réflexion européenne pour les ressortissants de l’Union Européenne.

L’apport du RGPD :

- renforcement du droit des personnes dont on traite les données. Exemple : l’information du traitement de données doit être lisible et compréhensible.
- responsabilisation de ceux qui traitent des données personnelles des ressortissants de l’Union Européenne. Exemple : la déclaration préalable à la CNIL a été supprimée, il s’agit d’avoir une réflexion concrète du professionnel pour sécuriser les données.

De quoi parle-t-on concrètement ?

“Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d’identification ou un ou plusieurs éléments qui lui sont propres.”

Projet soutenu par la Région Nouvelle-Aquitaine et l’Union Européenne dans le cadre du « Programme Opérationnel FEDER / FSE 2014-2020 »

Je traite de la donnée à partir du moment où je la collecte. Je l'enregistre dans un logiciel, sur un dossier, je consulte ma liste d'adhérents, je transmets ces informations à d'autres professionnels, je vais faire des modifications, rectifications, archiver cette donnée, voire je vais peut être supprimer la donnée. Toutes ces étapes relèvent du traitement des données à caractère personnel soumises au RGDP.

Une donnée sensible est une donnée à caractère personnel mais qui a un impact très important sur la personne, sur la vie privée, sur son intimité. Une nouveauté du RGPD qui en a fait une liste.

"Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, difficultés sociales de la personne, numéro de sécurité sociale, condamnation pénale.

Le règlement européen interdit de recueillir ou d'utiliser ces données, sauf, notamment, dans les cas suivants :

- si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;
- si les informations sont manifestement rendues publiques par la personne concernée ;
- si elles sont nécessaires à la sauvegarde de la vie humaine ;
- si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL ;
- si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale."

Quelles sont les obligations des professionnels ?

Je collecte que ce dont j'ai besoin > **minimisation**.

Je mets à jour ma liste de contact de ce professionnel partenaire > **obligation d'exactitude**.

Je récupère des données par une feuille d'émargement lors d'un événement, je vais lui dire ce que je vais faire avec ces données. Je ne vais pas réutiliser, donner ces élément à une autre entreprise sans l'autorisation de la personne > **obligation de loyauté et de proportionnalité**.

J'ai un objectif sinon je n'ai pas assez de justification pour traiter la donnée. Est-ce que j'ai nécessité à récupérer cette donnée ? > **détermination des finalités poursuivies**.

Je ne peux pas garder de manière indéterminée la donnée, je dois pouvoir mettre à jour et détruire la donnée > **fixation d'une durée de conservation des données**.

Projet soutenu par la Région Nouvelle-Aquitaine et l'Union Européenne dans le cadre du « Programme Opérationnel FEDER / FSE 2014-2020 »

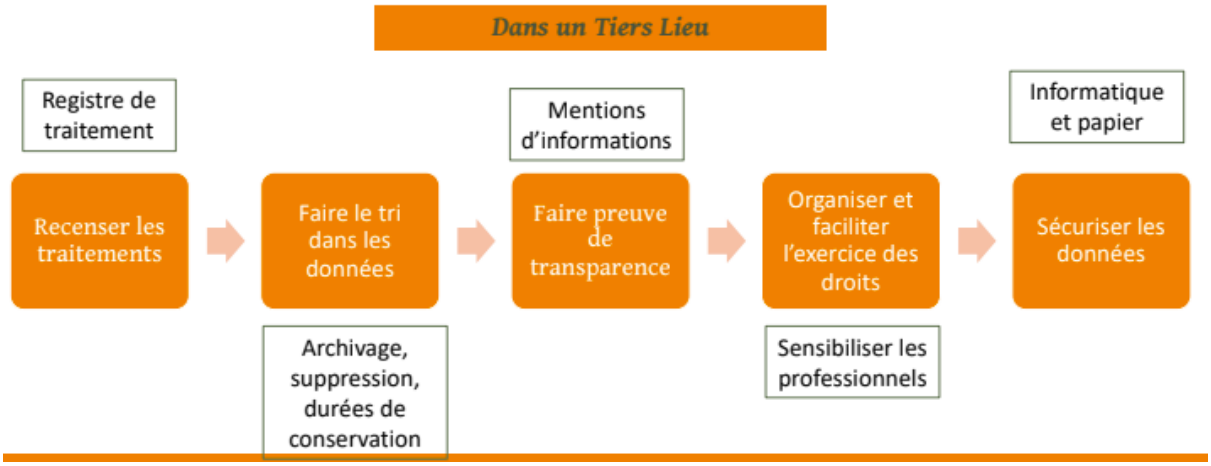
Le tiers-lieu est-il concerné ?

OUI ! Cela peut être les données de ses adhérent.e.s, de ses partenaires, de ses salarié.e.s, de ses stagiaires de la formation, des participants aux ateliers, des élus du conseil d'administration…

Où sont stockées les données personnelles du tiers-lieu ? Elles peuvent être stockées dans un cloud, un drive, des docs partagés mais où est-ce que ça va ? Souvent personne ne sait véritablement… L'objectif n'est pas de supprimer les outils mais d'avoir des outils qui permettent de protéger ces données. Elle peut aussi être stockée dans un ordinateur portable, un cahier à l'accueil, un portable professionnel, un tableau affiché au mur, des feuilles d'émargement…

Les données sont-elles protégées ? Où est le cloud, est-il sécurisé ? Est-ce que j'ai un antivirus ? Est-ce que le cahier est à la portée du public ? Est-ce que l'ordi est protégé par un mot de passe ? Il s'agit d'être dans le concret.

Les étapes de la mise en conformité



Questions

Notre financeur nous demande un niveau d'information tel que le statut de travail, chômage, bénéficiaire de minimas sociaux, est-ce une donnée sensible ?

C'est sensible mais justifié par la demande du financeur, il faut donc que la personne autorise activement l'utilisation de ces données. Une mention d'informations avec une case à cocher suivie d'une signature de la personne. Cela permet de la transparence (mention d'informations) et le recueil du consentement (case à cocher).

Exemple de mentions : "Conformément à la loi "informatique et libertés" du 6 janvier 1978 modifiée au Règlement européen n°2016/679/UE du 27 avril 2016 (applicable dès le 25 mai 2018), vous bénéficiez d'un droit d'accès, de rectification, de portabilité et d'effacement de vos données ou encore de limitation du traitement. Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant.

Projet soutenu par la Région Nouvelle-Aquitaine et l'Union Européenne dans le cadre du « Programme Opérationnel FEDER / FSE 2014-2020 »

Vous pouvez, sous réserve de la production d'un justificatif d'identité valide, exercer vos droits en contactant Mr ou Mme Prénom Nom, nom de la structure, au contact adresse@mail.

Pour toute information complémentaire ou réclamation, vous pouvez contacter la Commission Nationale de l'Informatique et des Libertés (pour plus d'informations sur www.cnil.fr)."

Nous avons un fichier récapitulatif des identifiants et mot de passe, est-ce risqué ?

Cela relève du RGPD, précisément de la sécurisation des données. Il faut également penser la continuité de service. Plusieurs personnes peuvent y avoir accès mais doivent s'engager sur une charte informatique sur les bonnes pratiques. Le mieux c'est d'avoir un coffre fort numérique.

Les données issues de la vidéo surveillance sont-elles liées au RGPD ?

Article de la CNIL relatif à la vidéosurveillance-vidéoprotection. Attention si cela empiète sur l'espace public.

Où sont stockées les données dans les répertoires téléphoniques ? Oui la liste de bénévoles est protégée mais les numéros de téléphone tout le monde les a.

Le principe du RGPD est "la circulation des données" tout en les protégeant. Il convient donc de trouver des moyens de protection adaptés au fonctionnement de la structure et en adéquation avec les cadre légal. En revanche, si j'ai conscience du caractère personnel des données de mon portable, c'est un lieu de stockage. Comment je sécurise mon téléphone ? Par exemple, si je me fais voler le téléphone, est-ce qu'on pourrait accéder aux informations et photos ? Je commence par sécuriser par un mot de passe, ensuite la structure s'engage à supprimer les numéros des adhérents et pro avec qui elle ne va plus travailler. Cela pourrait figurer dans la charte informatique. Il faut avant tout limiter le risque.

Quels types de contrôles sont exercés ? Que faut-il présenter ?

L'équipe de contrôle de la CNIL est pour l'instant composée d'une dizaine de personnes pour toute la France, toutes les structures, toutes les entreprises. Ses missions de contrôle s'organisent par secteur d'activité à raison d'un par an : formation, justice…

Le contrôle est tout à fait possible mais il y a des chances qu'il arrive plutôt suite à une réclamation auprès de la CNIL de la part du public de la structure. Les personnes sont informées et connaissent de plus en plus leurs droits. Si elles ont un doute, elles peuvent faire une réclamation à la CNIL.

L'enjeu est d'être respectueux des personnes.

Qu'est-il dit sur les services tels que mailjet ou sendinblue ?

Il faut être curieux pour analyser les lieux de stockage et la sécurisation des données. Ne pas hésiter à poser des questions.

Projet soutenu par la Région Nouvelle-Aquitaine et l'Union Européenne dans le cadre du « Programme Opérationnel FEDER / FSE 2014-2020 »

Les sous-traitants partagent une responsabilité avec ceux qui mettent en place une démarche.

Quelle gestion du droit à l'image ?

Article de service-public.fr relatif au droit à l'image et au respect de la vie privée.

Pour la diffusion du droit à l'image, il faut un consentement aussi bien la photo d'une personne que celle de l'organigramme des salarié.e.s. Le formulaire doit expliquer ce qui sera fait de la photo et que la personne consente à cela.

Notre projet de tiers-lieu rassemble des personnes touchées par un cancer du sein, aussi nécessairement de la donnée sensible va être manipulée dans l'activité de l'association. Quid ?

Si on recueille de la donnée anonyme on n'est pas dans le RGPD.

Dans le cas contraire, il faut sécuriser tout le parcours de la donnée et travailler sur le consentement des personnes ainsi que les échanges. Les structures sociales et médico-sociales ont des systèmes de plateforme d'échange des informations, pas simplement des mails.

Un.e ou plusieurs Délégué.e. à la Protection Données (DPO) ?

Dans les administrations publiques et structures qui traitent des données à grande échelle, la désignation d'un.e DPO est obligatoire. Aujourd'hui cela ne correspond pas, a priori, aux tiers-lieux mais un.e référent.e peut être désigné.e. Bien sûr, il.elle ne peut pas avoir la vue sur tout ce qui se passe au quotidien mais peut impulser la démarche, sensibiliser les équipes et faire des rappels.

Est-il possible de faire valoir la RGPD lorsque nous sommes démarchés par des entreprises qui passent par les contacts connus du grand public ?

Il peut être indiqué la requête de suppression par mail et indiquer que, si cela perdure, une réclamation à la CNIL sera réalisée.

Bonus

Support d'intervention de Virginie GIRAUD.

Sites et articles ressources :

- cnil.fr
- Comprendre le RGPD
- RGPD : de quoi parle-t-on ?
- L'obligation d'affichage en tiers-lieux

Documents ressources :

Projet soutenu par la Région Nouvelle-Aquitaine et l'Union Européenne dans le cadre du « Programme Opérationnel FEDER / FSE 2014-2020 »

- Guide de sensibilisation au RGPD pour les petites et moyennes entreprises
- FICHE 1 : Votre entreprise communique et/ou vend en ligne
- FICHE 2 : Améliorez et maîtrisez votre relation client
- FICHE 3 : Protégez les données de vos collaborateurs
- Modèle de registre des activités de traitement

Formation : La protection des données RGPD et mise en conformité (À DISTANCE) proposé par l'organisme de formation des tiers-lieux en Nouvelle-Aquitaine Trans//formations.

Projet soutenu par la Région Nouvelle-Aquitaine et l'Union Européenne dans le cadre du « Programme Opérationnel FEDER / FSE 2014-2020 »

PRÉFÈTE DE LA RÉGION NOUVELLE-AQUITAINE
Liberté
Égalité
Fraternité

FRANCE RELANCE

UNION EUROPEENNE

l'Europe s'engage en France

RÉGION Nouvelle-Aquitaine