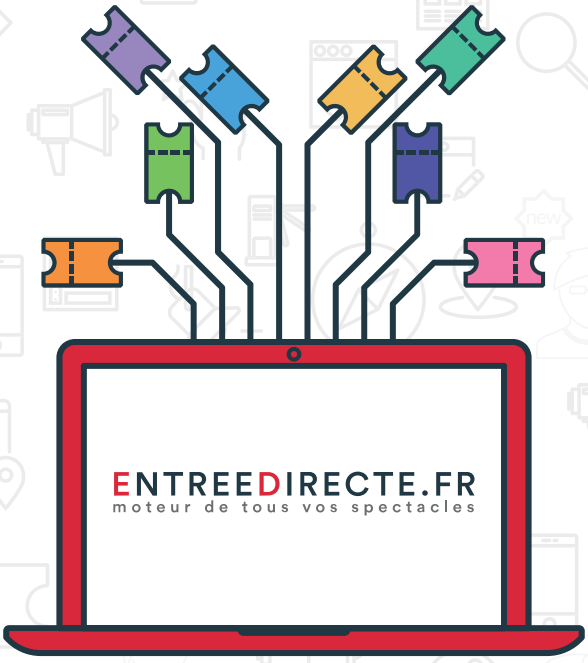
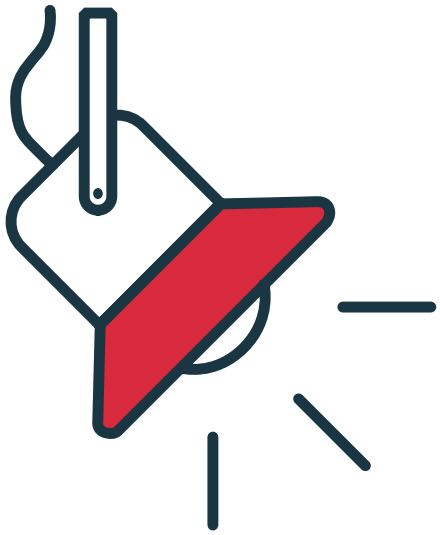
RGPD

« PETIT » GUIDE
À PROPOS DU RÈGLEMENT GÉNÉRAL
SUR LA PROTECTION DES DONNÉES
À L'USAGE DU SPECTACLE VIVANT



#spectaclepartout #spectaclepartous #spectaclepourtous

RÉFÉRENCEZ GRATUITEMENT VOS SPECTACLES



programme.entreedirecte.fr

EDprogramme est notre service innovant qui permet aux évènements peu médiatisés d'être référencés sur EDsearch et ainsi d'apparaître sur un pied d'égalité avec les programmations automatiquement référencées.

Ce formulaire interactif s'appuie sur un modèle de données unique et précis, parce qu'une bonne recherche commence par un bon référencement.

EDprogramme propose une qualification aiguisée des spectacles qui va bien au delà de la simple notion de genre et permet un véritable archivage pérènne et électronique de vos évènements.

référencez votre spectacle

AVANT-PROPOS

R, G, P et D, ces quatre lettres sont partout en ce moment. Elles sont souvent agrémentées de beaucoup d'informations indigestes, contradictoires, voir même alarmantes sur sa mise en place le 25 Mai 2018.

Halte au martelage cacophonique et place à un peu de sérénité dans ce monde connecté ! Les petites et moyennes structures de spectacle, les compagnies, les associations et les organisateurs ont déjà bien assez à faire pour ne pas se voir confier un énième défi digne d'un Sisyphe de la data.

Il se trouve que chez EntreeDirecte, la data, on adore ça ! Nous nous sommes donc lancées pleinement dans le périple du RGPD. Après avoir suivi une formation, questionné des avocats spécialistes, lu 486 pages, visité 32 sites web et bu 369 cafés, nous vous proposons ce guide qui tente de répondre aux problématiques posées par le RGPD au milieu du spectacle vivant.

Fait avec soin et amour, il a pour unique but de vous informer sur les mesures que nous pensons les bonnes pour vous mettre en conformité avec le RGPD. Vous restez néanmoins le seul et entier responsable légal de cette mise en conformité.

D'ailleurs, c'est « le » ou « la » RGPD ?

L'intitulé officiel est bien « le » Règlement sur la protection des données mais si vous aimez varier les articles, « la » Réglementation sur la protection des données, ça marche aussi.

Du côté des bonnes nouvelles, le RGPD ne change en somme pas grand-chose à ce que vous faîtes déjà.

Si vous êtes en conformité avec les lois préexistantes sur la donnée, **vous êtes compatible à peu près à 80% avec le RGPD**. Il n'est donc pas nécessaire dans beaucoup de cas de lancer une gigantesque campagne de mailing pour redemander à tous vos contacts la confirmation de leurs consentements à l'utilisation de leurs adresses. Il n'est pas non plus nécessaire de débourser tous les louis d'or de Molière en audits ou expertises.

Même si vous traitez des données personnelles en tenant des registres d'employés et que vous êtes un adepte de la newsletter pour donner son envol à votre belle programmation ; vous n'avez pas la taille ou les pratiques des GAFA[1] ou autres géants internationaux de la billetterie qui tracent leurs spectateurs partout sur internet ou sur un festival pour savoir comment ils achètent leurs places ou combien de litres de bière ils ont partagé avec tels amis devant telle scène... Enfin, si vous le faites on ne juge pas, hein ! Mais ce petit guide ne sera pas suffisant pour vous mettre en conformité de A à Z.

Cette mise en conformité avec le RGPD se fait étape par étape. Il n'est pas question de tout faire en trois jours. Il faut avant tout prioriser vos besoins et établir un plan d'action. Ce qui compte c'est de mettre en place les processus adéquats pour être aux normes.

Avec un peu d'huile de coude, cette mise en conformité est une incroyable occasion de valoriser votre image, améliorer votre base de données spectateurs, gagner en productivité et faire un brin de rangement administratif pour démarrer triomphalement votre prochaine saison !

Ah oui, nous allions oublier deux choses... Ce guide fait 56 pages. On sait que ça fait beaucoup à digérer mais pas d'inquiétudes, nous l'avons segmenté de façon claire et pratique que vous puissiez le consulter au gré de vos besoins. Si vous voulez partager, donner, recommander ou citer ce document, allez-y ! Nous serions ravies de voir que notre travail est utile. Par contre, ce document ne doit pas être modifié ou utilisé sans être cité comme source.

Pour toutes vos questions, commentaires ou avis c'est par ici : contact@entreedirecte.fr

Bon RGPD à tous !

L'équipe EntreeDirecte

[1] *Désigne quatre des entreprises les plus puissante du monde de l'Internet : Google, Apple, Facebook et Amazon*

SOMMAIRE

DEFINITIONS

QU'EST-CE QUE LA CNIL ?

La Commission Nationale de l'Informatique et des Libertés, est une autorité administrative indépendante chargée de **veiller à ce que l'informatique ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.**

QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

Toute information **identifiant directement** ou **indirectement** une personne physique. Elle peut prendre par exemple les formes suivantes :

- Nom, prénom
- Numéro d'immatriculation
- Numéro de téléphone
- Numéro de sécurité sociale
- Adresse mail
- Adresse postale/ commune de résidence / données de localisation
- Adresse IP
- Photographie
- Identifiant / pseudonyme utilisé en ligne
- Éléments spécifiques propres à l'identité d'une personne tels que l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale

QU'EST-CE QU'UNE DONNÉE SENSIBLE ?

C'est une donnée personnelle qui révèle :

- Les opinions politiques, philosophiques ou religieuses
- L'appartenance syndicale
- Les origines raciales ou ethniques
- La vie ou l'orientation sexuelle
- L'état de santé (physique et mentale)
- Les données biométriques
- Les données génétiques

Le traitement de ces catégories particulières de données est interdit (sauf autorisation explicite des personnes concernées et si le responsable du traitement a sollicité et obtenu une autorisation spécifique de la CNIL ou dans les cas spécifiques listés à l'article 9 du RGPD).

QU'EST-CE QU'UN FICHIER DE DONNÉES À CARACTÈRE PERSONNEL ?

N'importe quel **ensemble structuré de données personnelles et accessibles** est considéré comme un fichier de données à caractère personnel, donc soumis au RGPD. Exemples :

- Annuaire interne d'employés ou de spectateurs
- Suivi de demande de formation ou de congés
- Messagerie électronique
- Système de badgeage
- Gestion des déclarations d'accidents du travail et maladie professionnelle
- Base de données de CRM
- Outils de gestion de billetterie

QU'EST-CE QU'UN TRAITEMENT DE DONNÉES ?

Toute **opération automatisée ou non, appliquée à des données à caractère personnel**.

Les traitements visés par le RGPD sont évidemment les traitements informatiques mais aussi les traitements « **manuels** » ou « **papier** ».

Un ensemble de fiches, de listes ou dossiers structurés ou indexés, tel qu'un annuaire téléphonique papier ou les dossiers papier du personnel, constituent un traitement de données. Les procédés utilisés peuvent être :

- La collecte
- L'enregistrement
- La conservation
- La modification
- L'extraction
- La consultation
- La communication
- Le transfert
- L'utilisation
- L'interconnexion
- Le verrouillage
- L'effacement
- La destruction
- L'anonymisation

Le traitement de données doit avoir une finalité. On ne peut donc pas collecter ou traiter des données personnelles simplement au cas où elles pourraient s'avérer être utiles un jour !

QUI EST LE RESPONSABLE DU TRAITEMENT ?

Toute **entreprise ou structure qui collecte ou traite des données personnelles** et qui répond à l'un de ces critères :

- Une présence dans un pays européen.
- Pas de présence en Europe mais un traitement de données personnelles de résidents européens

Ces entreprises ou structures sont alors dénommées « **responsable du traitement** » bien que cette appellation ne désigne pas une personne physique.

QU'EST-CE QU'UN SOUS-TRAITANT ?

Toute **personne traitant des données à caractère personnel pour le compte du responsable du traitement** est considérée comme un sous-traitant dans le RGPD.

- Prestataire de paie, fournisseur de télécommunication.
- Prestataires de services informatiques (hébergement, maintenance, etc.).
- Intégrateurs de logiciels.
- Société de sécurité informatique.
- SSII
- Agence de communication (ex : gestion de la CRM des spectateurs).

Les éditeurs de logiciels ou fabricants de matériels n'ayant pas accès à la donnée **ne sont pas considérés comme sous-traitants**.

Voir la section dédiée à la sous-traitance en page 47.

QU'EST-CE QU'UN DPO ?

Le DPO (Data Protection Officer ou Délégué à la protection des données en bon français) est **une personne physique** qui assure le respect et le suivi du RGPD pour un responsable de traitement. Cette personne est un **référent** jouant également un rôle de **coordination** et sera le point de **contact entre la structure et la CNIL**.

Voir la section dédiée au DPO en page 23.

QUELS SONT LES DROITS DES PERSONNES DONT LA DONNÉE EST TRAITÉE ?

Une personne dont la donnée est collectée peut exercer les droits suivants, en contactant un **responsable de traitement qui sera alors dans l'obligation de lui fournir une réponse dans les meilleurs délais** (1 mois maximum) :

- Droit à l'information
- Droit d'accès à la donnée
- Droit de rectification
- Droit d'opposition
- Droit à l'oubli
- Droit à la limitation du traitement
- Droit à la portabilité des données
- Droit de recours en cas de non-respect

Voir le détail de ces droits en page 27.

QU'EST-CE QU'UNE FAILLE DE SÉCURITÉ ?

Toute atteinte à une base de données, c'est-à-dire les erreurs d'opérations, les bugs, les fraudes internes ou externes, le piratage, la perte ou le vol de données personnelles. Ces violations des données personnelles doivent faire l'objet de notification à la CNIL ainsi qu'aux clients et / ou partenaires et / ou personnes concernées dans les meilleurs délais.

Voir la section dédiée aux failles de sécurité en page 45.

QU'EST-CE QUI CHANGE POUR LES STRUCTURES AVEC LE RGPD ?

Auparavant, on devait envoyer à la CNIL des déclarations qui spécifiaient les processus de collecte et de traitement des données. Désormais il n'est plus nécessaire de les envoyer mais il faut toujours **tenir des registres et être en mesure de les mettre à disposition de la CNIL à tout moment**.

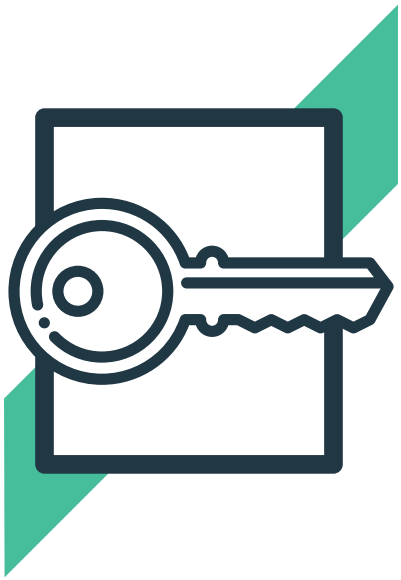
En ce qui concerne la mise en conformité permanente, le responsable du traitement doit s'assurer que des **mesures de sécurité pertinentes et appropriées** en fonction du traitement de données ont étés actées, sont appliquées et restent suffisantes tout au long de la vie du traitement.

Voir la section dédiée à la mise en conformité en page 17.

QUELLES SONT LES SANCTIONS PRÉVUES ?

La non-conformité d'un responsable de traitement avec le RDPG peut être sanctionnée par des amendes dont le plafond est fixé à **20 millions d'euros** ou **4% du chiffre d'affaires** mondial. La **responsabilité du sous-traitant** peut également être recherchée. Ces sanctions ont été relevées dans le but de s'assurer la mise en œuvre effective du RGPD, qui reprend des lois existantes actuellement peu ou pas respectées.

Des **sanctions pénales** peuvent être également mises en œuvre. Le non-respect du RGPD engendre un **risque pour votre image de marque et une perte de confiance** de vos spectateurs et partenaires.



PRINCIPES CLÉS DU RGPD

Voici les **grands principes** qui régissent le Règlement Général pour la Protection des Données :

- **Licité et loyauté :** Les traitements de données doivent correspondre à ce qui a été décrit aux personnes concernées, et respecter les règles du RGPD.
- **Limitation des finalités :** Les données personnelles collectées doivent avoir des finalités déterminées, explicites et légitimes.
- **Minimisation de données :** Les données collectées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire à un traitement prédéfini.
- **Exactitude :** Les données doivent être exactes et tenues à jour.
- **Limitation de la conservation :** Les données personnelles qui ne sont plus requises pour la finalité des traitements doivent être supprimées ou anonymisées.
- **Intégrité et confidentialité :** Le responsable de traitement doit garantir la sécurité de données collectées.
- **Responsabilité :** Le responsable du traitement doit être en mesure à tout moment de démontrer sa conformité avec chacun des principes énoncés ci-dessus.

Voici les quatre **champs d'action** majeurs que demande le RGPD :

- **Recenser :** Lister tous les fichiers, cartographier les traitements de données et établir un registre.
- **Trier :** Contrôler la nécessité des traitements, catégoriser ses données, vérifier les habilitations, et ne conserver uniquement ce qui est nécessaire.
- **Informer :** Mettre à disposition des utilisateurs les informations légales sur vos traitements de données, mettre en place des processus pour gérer l'exercice des droits des personnes dont les données sont collectées, et sensibiliser vos collaborateurs.
- **Sécuriser :** Garantir la sécurité des données, mettre à jour les logiciels et antivirus, vérifier les habilitations et les changements réguliers de mots de passe. Mettre en place des procédures en cas de violation de sécurité.

JOSÉPHINE BAKER À L'HEURE DU RGPD

Pour nous aider à envisager les formes que ces principes peuvent prendre au quotidien, nous avons choisi d'imaginer le cas de l'incroyable Joséphine Baker à l'heure du RGPD.

Joséphine est à la fois spectatrice, artiste et employée. À ce titre elle apparait dans différents types de fichiers : les fichiers spectateurs (B2C) des structures où elle va voir des spectacles, les fichiers artistes (B2B) des structures qui tiennent un registre d'artistes et autres prestataires, et enfin le fichier employée dans la structure avec laquelle elle a un contrat.

Voici donc la mise en pratique des principes clés du RGPD dans des exemples concrets qui vous parleront sans doute en tant que professionnels du spectacle vivant.

L'ensemble des règles qui régissent ces exemples est détaillé point par point dans nos fiches pratiques.

JOSÉPHINE, SPECTATRICE

Joséphine est une grande adepte du club du Vieux Colombier, qui a bien entendu une fiche « cliente » sur sa spectatrice. Celle-ci lui permet de conserver l'historique de ses achats, ses préférences en tant que spectatrice, ses coordonnées, un recueil de son consentement à la newsletter et enfin un zone de commentaire libre. Voici une comparaison entre une fiche licite et illicite:

FICHE SPECTATRICE

Prénom : Joséphine
Nom : Baker
E-mail : jojobaker75@gmail.com

Tarif préférentiel : - de 26 ans
Ville : Paris 9ème

Centres d'interêt
JAZZ THÉÂTRE DANSE CHANT

Consentement à la newsletter Oui - 3/8/1930

Commentaires
Impossibilité d'assister au spectacle du 12/12/28. Remboursement effectué. Abonnement familial régulier.
Préfère être contactée par E-mail.

FICHE SPECTATRICE

Prénom : Joséphine
Nom : Baker
E-mail : jojobaker75@gmail.com

Date de naissance : 3 juin 1906
Adresse : Hôtel Leman 20 Rue de Trévise, Paris 9

Centres d'interêt
ACTIVISME ÉROTISME DÉCADENCE

Inscrite à la newsletter

Commentaires
Insupportable au téléphone. Accent prononcé. D'origine ethnique. Célibataire. Très souvent dénudée.

Dans la fiche licite, on peut voir que seules les informations véritablement nécessaires sont consignées :

- Le Vieux Colombier n'a pas véritablement besoin de renseigner la date de naissance complète de Joséphine pour indiquer qu'elle bénéficie d'un tarif préférentiel.
- Puisqu'il n'envoie plus de programmation par la poste, pas non plus besoin de collecter son adresse postale, sa ville et son quartier feront l'affaire pour faire des statistiques de fréquentation.
- Les centres d'intérêt consignés doivent rester neutres.
- L'inscription à newsletter du Vieux Colombier doit être enregistrée sous la forme du recueil de consentement et comporter la date de celui-ci.
- Les commentaires libres doivent impérativement être neutres et ne jamais porter atteinte à l'image d'une personne.

JOSÉPHINE, ARTISTE

Mais Joséphine est bien plus qu'une spectatrice comme les autres, c'est aussi l'artiste la plus en vogue de son époque. De ce fait, beaucoup de salles de spectacle ont sa fiche professionnelle dans leurs registres car ils rêveraient ou ont déjà eu la chance de travailler avec la grande danseuse. C'est le cas du Théâtre des Champs Élysées qui pourrait avoir dans ses dossiers la fiche suivante :

FICHE ARTISTE

Prénom : Joséphine
Nom : Baker
E-mail : jbaker@audiffredandco.fr

Adresse : Agence Audiffred 2 rue puits, Paris 9
N° de Tél. pro : Bergère 28 32

Fonction : Chanteuse, Danseuse, Actrice
Compagnie : Dixie Steppers
Type de prestation artistique :
Danse exotique, revue burlesque, chorégraphie
Dernièrement contactée : 08/1930

Commentaires
Associée à Grace Kelly et Georges Simenon.
Bilingue.
Imprésario : Émile Audiffred
Disponible uniquement les week-ends.

FICHE ARTISTE

Prénom : Joséphine
Nom : Baker
E-mail : jojobaker75@gmail.com

Adresse : Hôtel Leman 20 Rue de Trévise, Paris 9
N° de Tél. perso : Wagram 72 10

Tarif : Trop cher
Comportement : Râleuse, toujours en retard.
Type de prestation artistique :
Refuse le dénudement intégral, pas de visite en loges
Dernier contact & type de mailing :
Pas de contact depuis plus de 3 ans, promotionnel

Commentaires
Sent le tabac, surfaite, trop «bronzée», ancienne espionne, enfant de la misère, pas d'enfant, lutte pour les droits civiques.

Voici les différences fondamentales entre une bonne pratique de collecte de data en B2B et une pratique peu vertueuse :

- L'adresse mail consignée dans la fiche licite est l'adresse professionnelle de Joséphine. Elle reste tout de même une donnée personnelle mais elle permet légalement au Théâtre des Champs Élysées de contacter Joséphine par mail, dans le cadre d'une relation B2B et sans avoir recueilli son consentement.
- L'adresse postale renseignée est son adresse professionnelle, en l'occurrence celle de son agence. Idem pour son numéro de téléphone. Un numéro de portable peut à la fois être professionnel et personnel mais un numéro de téléphone de domicile n'aurait pas vraiment de raison de se retrouver sur une fiche professionnelle.
- Dans la fiche illicite, ses prestations sont décrites de manières très négatives et portent atteinte à ses chances de travailler pour le théâtre. Il est important de ne pas porter préjudice à la personne dans ses formulations et de baser son référencement sur des éléments impartiaux.
- La zone de commentaire libre encore une fois est propice à de très nombreux débordements. Dans la fiche illicite, on trouve même ici des données sensibles donnant des indications sur l'origine sociale et ethnique de Joséphine, mais aussi sur sa vie privée et ses opinions politiques. Or le traitement de ces informations est formellement interdit.

JOSÉPHINE, EMPLOYÉE

Joséphine est également la fameuse meneuse de revue des Folies Bergère qui possèdent bien entendu un fichier « employée » à son sujet.

FICHE EMPLOYÉE

Prénom : Joséphine
Nom : Baker
E-mail : jo.baker@foliesbergere.fr

N° de Sécu : 2 0606 2B5XX XXXX XX
Titre de séjour : POAJ1LXXX

Fonction : Meneuse de revue
Casier judiciaire vérif. : Oui
CV
Notes de frais
Historique de badgeage

Commentaires
Arrêt maladie du XX/XX au XX/XX.
Ne mange pas de viande.
Chausse du 37, porte du 36

FICHE EMPLOYÉE

Prénom : Joséphine
Nom : Baker
E-mail : jojobaker75@gmail.com

N° de Sécu : 2 0606 2B5US 2757 12
Titre de séjour : POAJ1L1UK

Status : Syndicaliste chez FO
Casier judiciaire vérif. :
Arrêtée pour militantisme en 1955
CV
Notes de frais
Historique de badgeage

Commentaires
Hystérectomie en 1941. Mensuration : 90 - 64 - 90. Dépensière. Pas mariée. Adhérente au Parti communiste.

Ici, toute la difficulté réside dans le fait qu'un employeur est amené à avoir en sa possession beaucoup de données personnelles sur ses employés. Mais il doit veiller à ce que l'accès à ces informations soit limité au personnel qui en a véritablement besoin pour exercer ses fonctions, à ce qu'elles soient archivées correctement après un certain délai et à ce que les autres employés ne puissent pas découvrir des éléments de la vie privée de leurs collègues sur les serveurs internes.

- Pourquoi donner accès à tous sans restrictions à son adresse mail personnelle ? Joséphine est une vedette, elle pourrait être utilisée à tort par un employé un peu trop admiratif.
- Son numéro de sécurité sociale est une donnée personnelle, il ne doit pas être accessible par tous. Idem pour son visa.
- Son appartenance syndicale est une donnée sensible et ne doit pas être collectée.
- Ses notes de frais, ses déplacements et ses heures de badgeages sont des données personnelles et leurs consultations doivent être restreintes.
- En ce qui concerne la consignation d'information personnelle, il faut être très vigilant. Joséphine a subi une opération chirurgicale en 1941. Pour autant, les employés ne devraient en aucun cas savoir la nature de son arrêt maladie en tombant sur des documents disponibles à la vue de tous. Il en va de même pour ses mensurations. La costumière doit y avoir l'accès mais le responsable de billetterie n'a pas à les connaitre.

CHANTIERS À ENTREPRENDRE

Selon la taille et le fonctionnement de votre organisme, différentes actions peuvent s'avérer nécessaires ou tout simplement bénéfiques pour votre mise en conformité avec le RGPD. Le but de cette section est de vous proposer des étapes concrètes pour y parvenir.

1/ DÉSIGNER UN PILOTE (DPO)

Le DPO (Data Protection Officer ou délégué à la protection des données) est une personne physique nommée par le responsable de traitement pour piloter et garantir la conformité d'une structure avec le RGPD. Pour beaucoup de structure, il n'est pas obligatoire de nommer un DPO, mais il peut s'avérer être très utile de le faire. Nous avons consacré une fiche pratique à cet effet :

En savoir plus sur le DPO en page 23.

2/ RECENSER VOS TRAITEMENTS ET ÉTABLIR UN REGISTRE

Chaque structure de plus de 250 employés ou effectuant un traitement non occasionnel, présentant des risques pour les personnes ou portant sur des données sensibles ou condamnations pénales, doit être en mesure de mettre à disposition de la CNIL à tout moment un registre complet de ses traitements de données.

Les entreprises de moins de 250 salariés bénéficient d'une dérogation en ce qui concerne la tenue de registres complets. Elles doivent inscrire au registre les seuls traitements de données suivants :

- les traitements non occasionnels (gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.) ;
- les traitements susceptibles de comporter un risque pour les droits et libertés des personnes (exemple : systèmes de géolocalisation, de vidéosurveillance, etc.) ;
- les traitements qui portent sur des données sensibles (données de santé, infractions, etc.).

Les structures du spectacle effectuent un traitement de données à caractère personnel non occasionnel pour la gestion de la paie, de leurs clients et de leurs fournisseurs. Elles sont donc bien concernées par l'obligation de tenue de registres, même lorsqu'il s'agit de structures de moins de 250 employés.

Ces traitements non occasionnels serons par exemple un suivi des appels des spectateurs, une liste d'abonnés, un répertoire d'intermittents, des formulaires de contact et de vente en ligne ou au guichet, un enregistrement de mails pour l'envoi de newsletters, le stockage de données transactionnelles, un suivi de formation, ou encore un outil de paie.

Ce registre est un devoir, il doit donc être tenu formellement et contenir :

- Le nom et les coordonnées du DPO (si vous en avez un).
- Les différents traitements de données personnelles.
- Les catégories de données traitées.
- Les objectifs des traitements de données.
- Les acteurs (internes ou externes) qui traitent ces données ; vous devrez notamment clairement identifier les prestataires et les sous-traitants.
- Les flux, en indiquant l'origine et la destination des données, afin d'identifier les éventuels transferts de données hors de l'union européenne.
- Les durées de conservation des données.
- Une description générale des mesures de sécurité techniques et organisationnelles déployées.
- Une mention sur la localisation de vos données (serveur local, hébergé chez un tiers, dans le cloud, etc.)

Voici un exemple de modèle de registre proposé par la CNIL

Nous avons établi une liste de questions qui pourront vous aider à faire ce registre. Pour chacun de vos traitements, tentez de répondre à chacune des questions et de consigner les réponses dans un document.

Qui ?

- ☐ Qui est responsable de traitement, et qui est votre DPO (nom et coordonnées) ?
- ☐ Qui sont les responsables des services traitants les données dans votre structure ?
- ☐ Qui a accès à ces données ?
- ☐ Qui sont vos sous-traitants ?

Quoi ?

- ☐ Quelles catégories de données traitez-vous (Adresse ? Badgeage ? Abonnements réguliers ? etc.) ?
- ☐ Collectez-vous des données susceptibles de soulever des risques en raison de leurs sensibilités particulières ? (Par exemple, des données sur le handicap de spectateurs, sur la santé de vos employés ou encore sur des infractions dont vous auriez connaissance pour la gestion des jeunes publics) ?

Pourquoi ?

- ☐ Pour quelles finalités collectez-vous ou traitez-vous ces données ? (Gestion de vos publics, marketing, gestion de ressources humaines, sécurité, contrôle tarifaire, etc.)

Où ?

- ☐ Où sont hébergées vos données ? (Serveur dans vos locaux, chez un prestataire, dans le cloud ?)
- ☐ Vos données sont-elles stockées et/ou transférées dans d'autres pays ?

Ccombien de temps ?

- ☐ Combien de temps conservez-vous chacune de vos catégories de données ?

Comment ?

- ☐ Quelles sont les mesures de sécurité en place pour minimiser les risques d'accès non autorisés ?
- ☐ Quelles peuvent être les failles de sécurité et donc la violation de la vie privées des personnes ?

3/ PRIORISER LES ACTIONS

Une fois ce recensement effectué, le responsable de traitement doit s'assurer que :

- Seules les données strictement nécessaires sont traitées.
- L'analyse des traitements se fait dans la continuité, c'est-à-dire à la fois lors de la mise en place mais aussi tout au long de sa mise en œuvre.
- Que des mesures sont en place pour se conformer aux durées de conservations légales et sur l'archivage des données.

Voir fiches sur la collecte, la durée de conservation et l'archivage en page 29.

Une certaine attention est nécessaire si :

- Vous traitez des données sensibles.
- Vous traitez des données personnelles telles que la surveillance à grande échelle d'une zone accessible au public.
- Vous évaluez de façon systématique les aspects personnels de vos spectateurs ou employés.
- Vous prenez des décisions qui ont un impact juridique en se basant sur ces évaluations (par exemple, le profilage).
- Vous transférez des données hors de l'Union Européenne.

Dans ce cas, il est recommandé d'effectuer une **analyse d'impact** si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées.

Voir la section dédiée à l'analyse d'impact en page 25.

4/ ASSURER LA TRANSPARENCE ET L'INFORMATION

Le RGPD renforce l'obligation de transparence et d'information à l'égard des personnes dont vous traitez les données.

Que vos traitements soient de l'ordre interne (suivi des employés, notes de frais, trombinoscope, vidéo surveillance, etc.) ou externe (cookies sur vos sites web, mentions légales sur vos plateformes de vente en ligne, outil de CRM, liste d'email pour vos newsletters, etc.) il vous faut assurer que chaque personne dont la donnée est collectée soit clairement informée, et qu'elle puisse pleinement exercer ses droits.

Pour ce faire, il est important de comprendre les points suivants pour lesquels nous avons rédigé des fiches détaillées :

- Les droits à l'information, à l'opposition, à l'accès ou la rectification, à l'effacement, à la limitation de la collecte et à la portabilité des données. (Voir détail en page 27)
- La collecte et le consentement (Voir détail en page 35)
- Les mentions légales. (Voir le détail en page 43)
- Les cookies et les cookies Policy (Voir le détail en page 41)

5/ ORGANISER LES PROCESSUS INTERNES

Le responsable du traitement doit aussi mettre en place des procédures garantissant la protection des données à tout moment, et permettant de pallier à toutes les situations ou évènements qui peuvent se produire, telles qu'une faille de sécurité ou un changement de sous-traitant.

Cette organisation implique notamment :

- La prise en compte de la protection des données dès **la conception** d'une application ou d'un traitement.
- **La sensibilisation et l'organisation** de la remontée d'information en construisant notamment un plan de formation et de communication auprès de collaborateurs.
- **Le traitement** des réclamations et des demandes des personnes concernées quant à l'exercice de leurs droits en définissant les acteurs et les modalités.
- **L'anticipation** des violations de données en prévoyant, dans certains cas, la notification à l'autorité de protection de données dans les 72 heures et aux personnes concernées dans les meilleurs délais.

Voir la section dédiée aux failles de sécurité en page 45.

Voir la section dédiée aux sous-traitants en page 47.

Evaluer la sécurité des données personnelles de votre organisme

6/ DOCUMENTER LA CONFORMITÉ

Il est enfin essentiel de constituer un dossier documenté et à jour permettant de démontrer à tout moment à la CNIL que vos mesures organisationnelles et techniques sont conformes au RGPD.

Ce dossier devra comporter les éléments suivants :

- La documentation des traitements de données personnelles.
  - » **Le registre des traitements** (pour les responsables de traitements ou pour les sous-traitants),
  - » Et dans certains cas :
  - » les analyses d'impact sur la protection des données pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes
  - » l'encadrement des transferts de données hors de l'UE par le biais de clauses contractuelles types, règles internes d'entreprise (BCR) ou du Privacy Shield (si l'entreprise est américaine et y a adhéré).

- L'information des personnes.
  - » **Les mentions d'information,**
  - » les modèles de **recueil du consentement** des personnes concernées,
  - » **les procédures** mises en place pour l'exercice des droits des personnes.

- Les contrats qui définissent les rôles et les responsabilités.
  - » **Les contrats** avec les sous-traitants,
  - » les procédures internes en cas de **violations de données**,
  - » les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base.

FICHES PRATIQUES

LE DATA PROTECTION OFFICER OU DPO

Dans quel cas est-il obligatoire de nommer un DPO ?

L'article 37 stipule que la désignation d'un DPO par un responsable de traitement est uniquement obligatoire dans les cas suivants :

- S'il appartient au secteur public.
- Si son activité principale constitue un suivi régulier et systématique des personnes à grande échelle.
- Si son activité principale l'amène à traiter à grande échelle des données dîtes « particulières » ou « sensibles ».

La CNIL incite néanmoins fortement tous les organismes à nommer un DPO. Elle permet de confier à un « expert » l'identification et la coordination des actions à mener en matière de protection des données personnelles.

Le DPO n'est pas le responsable pénal, le responsable du traitement le reste dans tous les cas.

Pour une petite structure, il peut être très intéressant de mutualiser un DPO avec d'autres structures pour alléger les coûts et s'entraider dans la mise en conformité de cette industrie, avec toutes les problématiques et spécificités qui lui son propre.

Qui choisir comme DPO ?

Les organismes peuvent désigner un délégué interne ou externe à leur structure. Le délégué à la protection des données peut, par ailleurs, être mutualisé, c'est-à-dire désigné pour plusieurs organismes.

En revanche, le DPO ne peut pas être en conflit d'intérêt avec les autres missions exercées au sein de la structure, c'est-à-dire quand son poste ou son rattachement hiérarchique l'amène à prendre des décisions quant à la finalité et aux moyens de traitements des données.

Par exemple, les postes suivants ne peuvent être nommés DPO :

- Directeur General / Administrateur
- Directeur Opérationnel
- DAF
- DRH / Responsable des ressources humaines
- DSI
- Directeur marketing/ commercial
- Secrétaire General
- Responsable Billetterie

Quelles sont les missions du DPO ?

En tant que « chef d'orchestre » de la mise en conformité d'une structure, le DPO se doit :

- D'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés.
- De contrôler le respect du règlement et du droit national en matière de protection des données.
- De conseiller la structure sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution.
- De coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Quelles expériences peut-on attendre d'un DPO ?

Même s'il n'existe pas encore un profil type de DPO, certaines expériences sont en théorie propices à la réussite des missions qui lui seront confiées.

Une formation initiale en droit avec une spécialisation pour le droit des nouvelles technologies seraient idéales, ainsi qu'une formation pour le métier de DPO comme la certification du Bureau Veritas Certification. Mais cela varie selon la taille et le secteur d'activité des organismes.

PIA

Vue d'ensemble des obligations et de la méthode

0. Lancer un nouveau traitement

De nombreux services sont créés tous les jours dans le monde du numérique.

Qu'ils répondent aux besoins internes d'organismes ou à ceux de leurs clients, ces services reposent pour la grande majorité sur des traitements de données à caractère personnel.

Adressés à des groupes d'utilisateurs définis, ils collectent ces données à la volée lors de leur usage.

Stockées sur des serveurs, les données collectées sont vulnérables à différents risques : l'accès illégitime, la modification non désirée et la disparition.

Ces risques sont susceptibles d'avoir un impact important sur la vie privée des utilisateurs concernés.

1. Qualifier le traitement

Ces risques sont indésirables, aussi bien pour le responsable de traitement que pour les utilisateurs du service.

Ainsi, avant de lancer un traitement, il est important d'en faire une première analyse afin d'en déterminer les risques qu'il est susceptible d'engendrer.

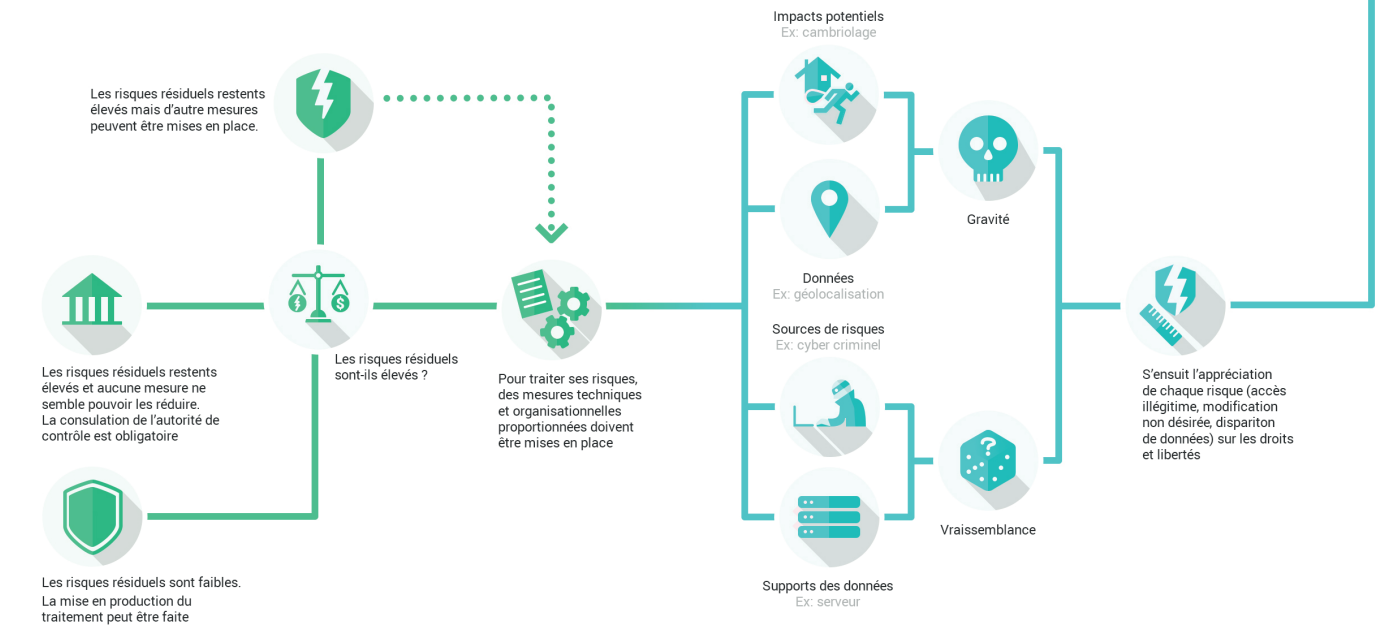
Plusieurs facteurs influencent la dangerosité d'un traitement comme par exemple le type de données traité.

En général, si deux des critères listés sont rencontrés, le traitement comporte probablement des risques importants sur la vie privée. Dans ce cas de figure, il est approprié de mener une *« analyse d'impact relative à la protection des données »*.

2. Apprécier les risques vie privée

L'analyse établit tout d'abord le contexte dans lequel évolue le traitement, en posant, entre autre, les bases de son rôle et de son fonctionnement.

En complément de l'étude juridique consistant à évaluer la nécessité et la proportionnalité du traitement, il est nécessaire d'analyser chaque risque et d'estimer sa vraisemblance et sa gravité selon les impacts potentiels sur les droits et libertés, les données traitées, les sources de risques, et les vulnérabilités des supports de données.



3. Traiter les risques

Une fois les risques identifiés, des mesures techniques et organisationnelles doivent être déterminées jusqu'à ce que les risques soient réduits à un niveau acceptable.

Si ça ne semble pas possible avec les moyens envisagés, l'autorité de contrôle doit être consultée.

Dans tous les cas, les mesures devront être appliquées avant la mise en œuvre du traitement.

Source : https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-dpia

L'ANALYSE D'IMPACT

Cette analyse d'impact est obligatoire lorsque les traitements remplissent au moins deux des critères suivants :

- Evaluation/scoring (y compris le profilage).
- Décision automatique avec effet légal ou similaire.
- Surveillance systématique.
- Collecte de données sensibles.
- Collecte de données personnelles à large échelle.
- Croisement de données.
- Données sur des personnes vulnérables (patients, personnes âgées, enfants, etc.).
- Usage innovant (utilisation d'une nouvelle technologie).
- Exclusion du bénéfice d'un droit/contrat.

Comment effectuer cette analyse d'impact ?

Les guides de la CNIL (en cours de révision à ce jour) décrivent la méthode suivante (Art. 35) :

1. Délimiter et décrire le contexte du (des) traitement(s) considéré(s).
2. Analyser les mesures garantissant le respect des principes fondamentaux : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées.
3. Apprécier les risques sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités.
4. Les mesures envisagées pour traiter ces risques et se conformer au règlement.

La CNIL propose un outil de PIA (Privacy Impact Assessment – ou analyse d'impact) pour faciliter la formalisation d'analyse d'impact :

https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

LE DROIT DE LA PERSONNE DONT LA DATA EST COLLECTÉE

Cette fiche vous donne le détail des articles du RGPD qui régissent le droit des personnes. Il est essentiel que ces droits soient assimilés par tous les collaborateurs car une fois que l'on sait quels recours ont les personnes pour accéder ou rectifier leurs données, on est bien plus attentif dans la mise en place de ses traitements.

Ces articles sont très formels, mais ne vous inquiétez pas, nous les avons remis dans le contexte des structures dans les autres fiches pratiques de ce dossier.

Droit à l'information (art. 13 & 14)

Toute collecte de données personnelles doit s'accompagner d'une information claire et précise des personnes avant la collecte sur :

- L'identité du responsable du traitement et les coordonnées du DPO le cas échéant.
- La finalité du fichier.
- La durée de conservation.
- L'existence d'un profilage.
- Le caractère obligatoire ou facultatif des réponses sur un formulaire.
- Les destinataires des données.
- Leurs droits (droit d'accès, de rectification, d'opposition, droit à l'effacement des données, droit à la limitation du traitement relatif à la personne concernée, droit à la portabilité des données, droit de retirer son consentement à tout moment, le droit d'introduire une réclamation auprès d'une autorité de contrôle).
- Les éventuels transferts de données vers des pays hors UE.

Le support de cette information varie en fonction des caractéristiques du fichier (exemple, panneau d'information pour une vidéosurveillance, mention d'information sur un formulaire, mentions légales sur un site web, lecture de cette information en cas de recueil de données par téléphone). Voir boîte à outils > Modèles de mentions CNIL

Droits d'accès et de rectification (art. 15 & 16)

Toute personne peut :

- Accéder à l'ensemble des informations la concernant.
- Connaître l'origine des informations la concernant.
- Accéder aux informations sur lesquelles le responsable du fichier s'est fondé pour prendre une décision la concernant (par exemple, les éléments qui auraient servi pour ne pas vous accorder une promotion ou le score attribué par une banque et qui a conduit au rejet de votre demande de crédit).
- En obtenir la copie (des frais n'excédant pas le coût de la reproduction peuvent être demandés).
- Exiger que ses données soient, selon les cas, rectifiées, complétées, mises à jour ou supprimées.

Droit à l'effacement (art. 17)

La personne dont la donnée est collectée a le droit d'obtenir l'effacement de ses données :

- Lorsqu'elle a **retiré son consentement** au traitement.
- Lorsqu'elle s'y **oppose**.
- Lorsque les **données ne sont plus nécessaires** au regard des finalités du traitement.
- Lorsqu'elles ont fait l'objet d'un traitement illicite.
- Lorsqu'elles doivent être effacées en vertu d'une **obligation légale**.

Droit à la limitation du traitement (art. 18)

La personne dont la donnée a été collectée a le droit d'obtenir la limitation du traitement plutôt que son effacement :

- Lorsqu'elle **conteste l'exactitude des données** et ce pendant une durée permettant au responsable de traitement de vérifier l'exactitude de ces données ;
- Lorsque le traitement est illicite, et que la personne concernée **s'oppose à leur effacement** et exige à la place la limitation de leur utilisation ;
- Lorsqu'elle en a besoin pour **la constatation, l'exercice ou la défense de ses droits en justice**.

Droit à la portabilité (art. 20)

Lorsque le traitement est fondé sur le consentement, ou sur un contrat, et effectué à l'aide de procédés automatisés, la personne concernée a le droit :

- De recevoir les données dans un **format structuré**, courant, lisible par machine et interopérable.
- De les **transmettre à un autre responsable du traitement** sans que le responsable du traitement initial y fasse obstacle.

Droit d'opposition (art. 21)

La personne concernée a le droit de s'opposer à tout moment au traitement des données, sauf lorsque celui-ci est nécessaire à l'exécution d'une mission d'intérêt public ou aux fins des intérêts légitimes du responsable du traitement.

Elle peut également s'opposer au traitement fait à des fins de prospection.

Ces droits peuvent s'exercer :

- **Par écrit :** par email ou courrier postal, accompagné d'une copie d'une pièce d'identité. Idéalement, en recommandé avec accusé de réception.
- **Sur place :** avec présentation d'une pièce d'identité. Il est possible de se faire accompagner par la personne de son choix. La consultation doit durer suffisamment longtemps pour prendre note commodément et complètement. Il est possible de demander une copie des données.

Quels sont les modalités de réponses ?

Le responsable du fichier dispose d'un délai de réponse maximal d'un mois (deux mois si complexité justifiable de réponse) à compter de la date de réception de la demande.

- Si la demande ne peut être satisfaite immédiatement, un avis de réception daté et signé doit être remis au demandeur.
- Ces demandes doivent être gratuites.
- Le responsable peut refuser la demande si elle est manifestement infondée ou excessive, notamment par leur nombre, leur caractère répétitif ou systématique.
- Si la demande est incomplète, le responsable du fichier est en droit de demander des compléments : le délai est alors suspendu et court à nouveau une fois ces éléments fournis.
- Lorsque le responsable de fichier ne dispose d'aucune donnée sur la personne qui exerce son droit d'accès (ex : les données ont été supprimées ou l'organisme ne dispose d'aucune donnée sur la personne), il doit néanmoins répondre au demandeur dans un délai de deux mois.
- Les éléments communiqués doivent être aisément compréhensibles. Les codes, les sigles et les abréviations utilisés doivent être expliqués (éventuellement par le biais d'un lexique). Par exemple, une mention explicative telle que « Segmentation : A+ » signifie que vous êtes considéré comme un spectateur VIP.

DURÉE DE CONSERVATION DES DONNÉES

Les durées de conservation sont un vaste sujet ! En effet, à chaque base de données ses règles. Voici donc les deux types de bases les plus couramment utilisées dans vos relations avec vos publics.

La première, c'est votre base de **prospect**, c'est-à-dire les personnes dont vous avez légitiment collecté l'adresse sans pour autant qu'ils soient vos clients. Dans ce cas, la règle pour la conservation des données était jusqu'à présent simple: trois ans à compter de la collecte de la donnée ou du dernier contact émanant du prospect.

Cette recommandation émanait de la Norme Simplifiée n°48 qui a été déclarée sans valeur juridique par la CNIL à compter du 25 mai 2018. En conséquence, nous ne pouvons pas savoir quelle sera la durée de conservation conseillée.

En ce qui concerne **vos spectateurs possédant un compte client chez vous** ; il vous appartient en tant que responsable de traitement de définir un délai à partir duquel ce compte doit être considéré comme inactif. Il faudra alors informer l'utilisateur de l'échéance de son compte utilisateur et lui donner la possibilité de s'opposer à la suppression de son compte client. Si vous n'obtenez pas cette opposition, il conviendra de le supprimer ou de l'archiver de façon intermédiaire (voir fiche sur l'archivage).

A noter qu'un clic sur un lien hypertexte contenu dans une newsletter **est une forme de contact**. Par contre, l'ouverture d'un mail **ne peut être considérée** comme un contact émanant du prospect.

Voici une liste des durées de conservation comme autrefois préconisées par la CNIL et qui nous ont semblées les plus pertinentes à titre d'exemple pour votre secteur d'activité. La liste complète est disponible dans notre boîte à outils > Dossier CNIL «Référenciel de durée de conservation des données» :

Ressources humaines :

- **Gestion du personnel : 5 ans** (en archivage intermédiaire) à compter du départ du salarié.
- **Gestion de la paie : 5 ans** à compter du versement de la paie.
- **Fichiers de recrutement :** Destruction immédiate si le candidat n'est pas retenu ni pour le poste à pourvoir ni dans le cadre d'un futur recrutement. Possibilité de conserver le CV pendant **2 ans** après le dernier contact avec le candidat.
- **Vidéosurveillance : 1 mois**.
- **Contrôle des horaires :** Les éléments d'identification ne doivent pas être conservés au-delà de **5 ans** après le départ du salarié ou de l'agent de l'entreprise ou de l'administration.
- **Contrôle d'accès : 3 mois** (historique des passages)

Fichiers commerciaux et marketing :

- **Les contrats conclus entre commerçants ou entre commerçants et non commerçants : 5 ans** Lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à 120€. Le contractant professionnel assure la conservation de l'écrit qui le constate pendant 10 ans.
- **Gestion des commandes / livraisons / facturation / comptabilité : 10 ans.**
- **Gestion d'un fichier client :** Les données des spectateurs sont conservées pendant le temps de la relation commerciale. Elles peuvent être conservées à des fins de prospection commerciale au maximum pendant **3 ans** à compter de la fin de cette relation commerciale. Ces délais sont amenés à évoluer.
- **Constitution et gestion d'un fichier de prospects : 3 ans** à compter de leur collecte par le responsable de traitement ou du dernier contact **émanant** du prospect.
- **Statistiques de mesures d'audience :** Les informations stockées dans le terminal des utilisateurs (exemple : cookies) ou tout autre élément utilisé pour identifier les utilisateurs et permettant la traçabilité des utilisateurs ne doivent pas être conservés au-delà de **13 mois**. Cette durée pouvant être amenée à évoluer avec l'entrée en vigueur du règlement «e-privacy» aujourd'hui en discussion.
- **Gestion d'une newsletter :** Jusqu'à **désabonnement** de la personne concernée ou **3 ans** à compter de la dernière interaction avec le prospect ou de la fin de la relation commerciale avec le client.
- **L'envoi de sollicitations (emailings, appels téléphoniques, télécopies, SMS, etc.) : 3 ans** à compter de leur collecte par le responsable de traitement ou du dernier contact **émanant** du prospect.

ARCHIVAGE DES DONNÉES

Les données personnelles doivent être conservées uniquement le temps nécessaire à l'accomplissement de la finalité poursuivie lors de la collecte et selon des durées maximales telles que définies dans la fiche «Conservation des données»

La CNIL distingue trois étapes dans la conservation des données :

- **Les bases actives ou archives courantes :** il s'agit des données d'utilisation courante par les services en charge de la mise en œuvre du traitement (par exemple votre base de données spectateurs, votre base de données prestataires, votre base de données de comptabilité, etc.)
- **Les archives intermédiaires :** il s'agit des données qui ne sont plus utilisées mais qui présentent encore un intérêt administratif pour l'organisme. Les données sont conservées sur support distinct et sont consultées de manière ponctuelle et motivée (l'enregistrement de transactions, vos données de facturation, etc.)
- **Les archives définitives :** il s'agit des données présentant un intérêt historique, scientifique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction. Elles sont alors régies par le livre II du Code du patrimoine et plus par la loi « informatique et libertés ».

A chaque étape, différentes techniques et processus existent pour minimiser la sensibilité des données, se conformer au devoir d'effacement sans supprimer toute sa base de données en anonymisant ou encore en pseudonymisant ses données.

Anonymisation (art.11 / considérant 26 et 57)

L'anonymisation est une opération qui consiste à transformer des données personnelles de façon à ne plus permettre l'identification de la personne concernée.

Cette transformation doit être irréversible. C'est-à-dire qu'il ne doit pas exister de méthode directe ou indirecte permettant de rattacher les données à la personne d'origine.

Les données comportant des informations à caractère personnel peuvent être conservées au-delà des délais de détention autorisées par la CNIL si elles sont convenablement anonymisées.

Cette technique est également utile pour transmettre tout ou partie du jeu de données à un tiers qui aurait besoin de travailler sur les données réelles sans avoir besoin des données nominatives.

Par exemple, vous pouvez vouloir analyser la fréquentation de votre salle les dix dernières années en utilisant vos données spectateurs. Or vous ne pouvez pas les conserver telles quelles plus de 3 ans en base active et 5 ans en archive avec un accès restreint.

L'anonymisation vous permettra alors d'analyser les âges de vos spectateurs, la distance moyenne parcourue pour venir dans votre salle, etc. car il sera impossible d'identifier ces spectateurs.

Cela peut aussi avoir un intérêt en base courante en interne afin que votre service comptable ait accès à certaines informations pour l'analyse de documents mais sans que la donnée personnelle de vos employés soit consultable par tous.

On pourra distinguer deux types d'anonymisation :

- **L'anonymisation à bref délai :** les données personnelles sont collectées puis anonymisées quelques secondes après. En raison de ce délai très court pendant lequel les données ne sont pas anonymes, le responsable de traitement bénéficie d'une obligation d'information alléguée : il doit indiquer son identité et la finalité du traitement. C'est le cas par exemple pour des opérations de paiements avec les données bancaires.
- **L'anonymisation ultérieure :** ce procédé permet, une fois le délai de conservation atteint, de ne pas supprimer les données personnelles (pour les conserver à des fins statistiques par exemple). Jusqu'à cette anonymisation, les données doivent avoir été collectées et traitées dans le strict respect de la Loi de 1978.

Pseudonymisation (art.4, 6, 25, 32, 40 et 89 / considérants 28, 78 et 156)

On peut vouloir rendre illisible une donnée personnelle tout en voulant être en mesure de la rendre lisible à nouveau.

Puisque l'anonymat est irréversible, on parlera de « pseudonymat».

Un des intérêts du pseudonymat est de réduire la surface du risque.

La masse des données étant pseudonymisées, leur stockage et leur traitement ne nécessite pas de protection supplémentaire par rapport à la sécurité conventionnelle. Seules les données et le mécanisme de lever du pseudonymat, ainsi que les traitements qui les utilisent, doivent bénéficier d'un surcroît de sécurité.

Par exemple, un théâtre peut explorer des données de navigation et en extraire une liste de prospects sous la forme d'une collection de pseudonymes d'adresses emails. C'est uniquement au moment de l'envoi de la campagne qu'un composant spécifique et protégé remplacera le pseudonyme par la valeur réelle.

Mise en garde

L'anonymisation est très tentante pour les structures, car l'analyse et la segmentation de leurs données est absolument capitale pour la compréhension des publics.

Or il est très courant que les risques de réidentification soient sous-estimés car il est facile pour un hacker de retrouver l'identité d'origine affiliée à vos données si les mesures de sécurité qui s'imposent ne sont pas prises.

Méthodes

La suppression :

La méthode la plus facile pour anonymiser vos données reste d'effacer les données sensibles.

Dans une base de données, on remplacera la valeur voulue par NULL (signifiant l'absence de valeur). Si toutes les valeurs permettant la réidentification ont bien été supprimées, alors l'anonymisation est garantie.

Cette solution n'est parfois pas déployable pour des raisons de fonctionnement de votre base de données. Par exemple si les champs que vous voulez anonymiser sont obligatoires ou que l'absence de valeur puisse perturber le bon fonctionnement de vos outils.

La mise à blanc :

Si on ne peut pas aisément supprimer la valeur d'un champ, on peut remplacer la valeur que l'on veut anonymiser par une valeur prédéfinie et constante, qui n'aura absolument aucune signification. Cela revient à utiliser la méthode de recouvrement au marqueur noir sur les fichiers papiers.

On peut utiliser des blancs, des underscores « ___ » ou encore des croix « XXXX ».

Troncature :

Pour tronquer une information, il faut en réduire la précision en conservant par exemple uniquement les premières lettres d'un nom, ou en ne conservant que l'année de naissance plutôt que la date complète d'un spectateur.

Attention à ne pas avoir recours à des initiales, qui sont très faciles à identifier une fois remises dans un contexte ! Par exemple : JMR du RP a discuté avec OP du FA 2018… Avec un peu de contexte, tel que « directeur de théâtre parisien » et « festival à Avignon » il devient facile de deviner de qui il peut s'agir.

La substitution

La substitution consiste à remplacer les données par une autre valeur qui n'a aucun rapport avec la valeur d'origine. C'est l'une des méthodes les plus efficaces pour appliquer le masquage des données.

Par exemple, si vous traitez des données source qui contiennent des enregistrements de spectateurs, le nom de famille réel ou le prénom peut être substitué de manière aléatoire à partir d'un fichier de recherche fourni ou personnalisé.

Si le premier passage de la substitution permet d'appliquer un prénom masculin à tous les prénoms, alors le second passage devrait permettre d'appliquer un prénom féminin à tous les prénoms où le sexe est égal à « F ».

En utilisant cette approche, nous pourrions facilement maintenir la mixité au sein de la structure de données, appliquer l'anonymat aux enregistrements de données mais également maintenir une base de données réaliste qui ne pourrait pas facilement être identifiée comme une base de données masquée.

Chiffrement

Le chiffrement est une forme de Pseudonymation qui remplace la valeur d'origine par une valeur illisible sans la clé de déchiffrement. Contrairement à la substitution, le secret se limite à la seule clé de déchiffrement, ce qui en simplifie encore la gestion et la sécurisation. L'anonymisation est possible en oubliant la clé de déchiffrement, mais elle ne peut être partielle.

Hachage

Le hachage est la transformation d'une chaîne de caractères en valeur ou en clé de longueur fixe, généralement plus courte, représentant la chaîne d'origine. Il permet de calculer une empreinte (ou signature) unique à partir des données fournies. Elle ne permet pas de retrouver la valeur originelle sans conserver un dictionnaire.

CRÉER UN COMPTE

email@domaine.com

••••••••

valider

☐ J'accepte de recevoir par voie électronique, de la part de la structure, des informations et / ou des offres préférentielles sur ses spectacles / produits.

☐ J'accepte de recevoir des informations ou offres promotionnelles des partenaires.

Vous pouvez vous désinscrire à tout moment en modifiant les paramètres sur votre compte et à travers les liens de désinscription. Les données à caractère personnel communiquées ici sont collectées par XX, traitées et conservées pendant une durée de X (X) ans à compter de XX, dans le seul but de X.

Conformément à la réglementation en vigueur, vous disposez du droit de demander l'accès à vos données à caractère personnel, la rectification ou l'effacement de celles-ci, une limitation du traitement qui vous concerne, du droit de vous opposer audit traitement ainsi que du droit à la portabilité de vos données en contactant XX par courrier électronique à l'adresse suivante : contact@xx.fr.

CRÉER UN COMPTE

email@domaine.com

••••••••

valider

☑ Je souhaite recevoir les offres de vos partenaires par voie électronique.

CRÉER UN COMPTE

email@domaine.com

••••••••

valider

☐ Je ne souhaite pas recevoir vos offres, ainsi que celles de vos partenaire par voie électronique.

INSCRIPTION NEWSLETTER

email@domaine.com

valider

En indiquant votre adresse e-mail ci-dessus, vous consentez à recevoir notre lettre d'information sur notre programmation. Vous pouvez vous désinscrire à tout moment en utilisant le lien de désabonnement intégré dans la newsletter.

INSCRIPTION NEWSLETTER

email@domaine.com

valider

En vous inscriviant à la newsletter, vous recevez une remise immédiate sur vos prochains billets de spectacle.

En acceptant nos CGU, vous acceptez l'envoi d'offres commerciales par voie électronique.

COLLECTE LORS D'UN RENSEIGNEMENT DE CHAMPS DE COMMENTAIRE LIBRE

Il est important de souligner le danger des zones de commentaires libres dans les outils et formulaires. En effet, on les trouve souvent un peu partout au sein des organisations (agenda de contacts, gestionnaires de tâches, observations, notes manuscrites, etc.). Et même si elles ne semblent pas appartenir au sujet du RGPD de prime abord, ces zones permettent de connaître un spectateur ou un prestataire.

Il faut donc veiller à ce que les informations collectées dans ces champs de commentaires libres ne portent jamais atteinte à l'image de la personne.

- Les commentaires doivent donc rester neutres, proportionnés et objectifs.
- Ils ne doivent jamais comporter d'indication de données sensibles.
- Il faut constamment garder en tête le droit d'accès à cette donnée que la personne peut exercer.
- Il faut impérativement sensibiliser et former les collaborateurs à ces problématiques.

Prenons un exemple concret, un spectateur demande un remboursement de billets car son partenaire est hospitalisé pour un cancer. Il est important de comprendre l'exception qui pourrait conduire une structure à rembourser le spectateur. Pour autant, il ne doit être mentionné nulle part les raisons précises qui conduisent à cette exception. Il sera plus judicieux de signifier une « impossibilité » du spectateur dans les registres de remboursement ou dans la fiche du spectateur.

COLLECTE DE DONNÉES SUR VOTRE SITE VITRINE

Vous avez sans doute un site vitrine qui présente votre programmation, votre histoire, vos équipes, etc. Et vous avez sans doute également dans ce site un formulaire de contact et la possibilité de s'inscrire à votre newsletter. Dans ce cas, il vous faudra :

- Indiquer les mentions légales CNIL en bas du formulaire de contact (voir boîte à outils)
- Une adresse de contact pour que les personnes puissent exercer leurs droits par voie électronique.
- Les mentions légales identifiant l'éditeur du site (voir boîte à outils).

Pour être certain de votre conformité lors des inscriptions aux newsletters, vous pouvez ajouter en dessous du champ de saisie de l'adresse une mention de ce type, à personnaliser selon vos besoins :

En indiquant votre adresse email ci-dessus, vous consentez à recevoir notre lettre d'information sur notre programmation. Vous pouvez vos désinscrire à tout moment en utilisant le lien de désabonnement intégré dans la newsletter.

L'inscription à une newsletter ne doit jamais être conditionnée. Le téléchargement de votre programmation ou l'accès à votre site sous réserve d'inscription à votre newsletter est donc interdit !

COLLECTE DE DONNÉES LORS DE LA VENTE EN LIGNE

Vous avez peut-être une plateforme de billetterie en ligne qui vous permet de vendre vos places ou vos abonnements par l'intermédiaire d'un formulaire. Ce formulaire vous permettant de collecter un grand nombre de données personnelles, il faut impérativement que :

- L'ensemble du parcours d'achat soit en https.
- Les champs obligatoires et facultatifs soient différentiés à l'aide d'astérisques ou de mentions du type « facultatif » / « optionnel » pour que l'utilisateur sache clairement ce qui lui est nécessaire ou non de renseigner.
- Un mot de passe suffisamment complexe soit demandé s'il y a une création de compte.
- Vous ne conserviez pas les données bancaires de vos acheteurs, sauf accord spécifique de leur part.
- Les transactions soient sécurisées.

- Les données que vous collectez dans ces formulaires soient justifiées par le service rendu au spectateur.
- L'information sur l'utilisation des données soit claire et accessible sur une page « Vie Privée ».
  (Voir la fiche «Les mentions sur votre site»)
- Le consentement de vos spectateurs à l'utilisation de leurs données soit explicite.
- Les spectateurs puissent aisément vous contacter au sujet de leurs droits.

On peut se demander par exemple s'il est légitime de demander la date de naissance d'un spectateur ?

- Pour un tarif préférentiel, le billet ne sera sans doute pas envoyé ou remis sans justificatif. La demande de la date de naissance à donc peu d'intérêt. Si vous la demandez pour des statistiques, pour ne pas se contenter d'une tranche d'âge ou d'une année de naissance ?
- Si vous gérez un spectacle interdit au moins de X années la collecte de la date de naissance peut avoir un intérêt légal.
- Si vous offrez un service particulier à vos spectateurs le jour de leur anniversaire (tel que des remises), vous pouvez proposer le renseignement de ce champs facultatif, en explicitant bien à quelles fins vous utiliserez cette information dans vos mentions légales.

Lorsque vous collectez les adresses de vos spectateurs lors de ventes par téléphone ou au guichet, pensez à prévoir un document et/ou discours type que vous afficherez et/ou reciterez à vos spectateurs lors de la collecte.
Voir boîte à outils > Modèles de mentions CNIL

LES BASES DE DONNÉES D'E-MAIL

Les newsletters sont l'objet de toutes les attentions ces dernières semaines. L'afflux massif d'emails demandant que vous confirmiez votre inscription à une newsletter est parfois envoyé à tort. Les informations disponibles sont souvent contradictoires, reprenons alors les éléments de compréhension depuis le début, pour bien différentier ce qui doit être fait de ce qui n'est pas obligatoire.

Qu'est-ce que le B2B et le B2C ?

Le **B2B** (Business to Business) désigne **l'ensemble des activités commerciales entre deux structures**. Le B2B concerne donc tous les moyens utilisés pour mettre en relation ces structures et faciliter les échanges de produits, de services et d'informations entre elles. Une adresse mail B2B sera alors du type prenom.nom@nomdelorganisme.fr. Elle est considérée comme une donnée personnelle car affiliée à une personne physique.

Le **B2C** (Business to Consumer) désigne quant à lui **l'ensemble des relations entre les structures et leurs publics** ainsi que les moyens techniques ou logiciels utilisés pour faciliter les interactions entre des professionnels et le grand public. Une adresse mail B2C prendra la forme prenom.nom@fournisseurdemessagerie.fr, c'est une donnée personnelle.

NOTE : Une adresse mail générique du type contact@nomdelastructure.com n'est pas considérée comme une donnée personnelle. LE RGPD n'est donc pas applicable à ce type d'adresse.

La collecte et l'utilisation d'adresse mail pour l'envoi d'email et de campagne

Regardons maintenant les règles à suivre pour collecter et utiliser légalement ces adresses pour vos campagnes.

En B2B, vous n'avez **pas besoin de recueillir le consentement** d'un professionnel de votre milieu si :

- **La sollicitation de votre mail est en rapport avec la profession de la personne démarchée.**
- **La collecte a lieu à l'occasion d'une vente ou prestation de services.**
- Le doit d'opposition est respecté avec un opt-out (lien de désinscription) dans les envois.
- Une information claire sur les conditions de traitement des données est disponible lors de la collecte (Mentions légales / Privacy Policy / Formulaire de collecte). Voir la fiche «Les mentions sur vos sites»
- Vous ne transmettez pas ces données à un tiers sans consentement explicite.
- Vous ne conservez pas ces données en base active passé le délai de 3 ans, si vous n'avez eu aucun contact ou interaction avec cette personne. Voir la fiche «Conservation des données»

En **B2C**, vous **devez recueillir le consentement** d'une personne pour collecter et utiliser son adresse pour recevoir des offres de votre part. Vous serez conforme au RGPD si :

- **Vous obtenez le consentement explicite de la personne avec un opt-in (case à cocher) lors de la création d'un compte ou d'un achat.**
- **Vous obtenez le consentement par une inscription directe à votre newsletter.**
- Le droit d'opposition est respecté avec un opt-out (lien de désinscription) dans les envois.
- Une information claire sur les conditions de traitement des données est disponible lors de la collecte (Mentions légales / Privacy Policy / Formulaire de collecte). Voir la fiche «Les mentions sur vos sites»
- Vous ne transmettez pas ces données à un tiers sans consentement explicite.
- Vous ne conservez pas ces données en base active passé le délai de 3 ans, si vous n'avez eu aucun contact ou interaction avec cette personne.

Cela veut donc dire que des mentions et consentements doivent être mises en place en interne, au guichet, par téléphone et sur vos sites) comme nous l'avons défini dans les sections dédiées à la collecte de données. Voir boîte à outils > Modèles de mentions CNIL

LA MISE A JOUR DE VOTRE BASE DE DONNÉES D'EMAIL

Revenons-en à cette vague de mails nous demandant de confirmer une inscription pour se mettre en conformité avec le RGPD. Ont-ils vraiment tous un fondement légal et vous faut-il faire de même ?

Cela peut avoir un intérêt si :

- Vous souhaitez profiter du RGPD pour requalifier votre base de données en n'y conservant que les emails des personnes activement intéressées par vos envois.
- Vous savez votre historique de collecte peu vertueux.
- Vous pensez que deux précautions valent mieux qu'une.

En travaillant dans le spectacle vivant, il est probable que la plupart des adresses mail présentes dans votre base de données active ait été collectées lors de l'achat de billets ou lors d'une inscription à votre newsletter. Ce motif de collecte est donc légitime.

De plus, la Loi informatique et libertés modifiée en 2004 stipule :

> *Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :*
>
> 1. *Le respect d'une obligation légale incombant au responsable du traitement ;*
> 2. *La sauvegarde de la vie de la personne concernée ;*
> 3. *L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement*
> 4. *L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;*
> 5. *La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.*

Ce qui veut dire que si un spectateur a acheté un billet en ligne et que vous avez collecté son adresse lors de cette vente, vous devez sans doute déjà avoir en place un recueil de consentement, cette loi datant de 2004.

Il en va de même pour les adresses collectées par le biais d'une inscription à une newsletter.

La réglementation en matière d'information à la personne dont la donnée est collectée est plus stricte et complète de nos jours, mais n'est pas pour autant rétroactive.

Il est sans doute plus difficile de savoir si vous n'avez pas eu de contact ou d'interaction avec ces personnes depuis plus de trois ans, mais si votre newsletter contient un lien de désabonnement, elles ne se sont pas non plus désinscrites.

Dernièrement, si vous n'avez jamais eu le droit véritable de contacter ces personnes, en toute logique vous n'auriez pas non plus le droit de le faire aujourd'hui via un email qui demande de confirmer une inscription. C'est donc une fausse solution.

Le vrai problème est de savoir à quand remonte la collecte de la donnée au sein de la structure. Il n'y a souvent pas de protocole établi pour dater cette collecte.

Cela ne veut pas dire que votre base de mailing ait été collectées de manière illicite.

Ce qui est important, c'est d'être en mesure de prouver à la CNIL que vous avez pris les mesures nécessaires dès à présent pour vous mettre en conformité sur le plan de l'enregistrement du consentement et des dernières dates d'interactions avec vos spectateurs.

Pour cela nous préconisons **à titre d'information** la checklist suivante pour mettre votre base de données en conformité dès aujourd'hui sans avoir à passer par une campagne de confirmation d'inscription:

- ☐ Effectuer un tri dans votre base de données. Si le vous pouvez, supprimez toutes les adresses que vous savez inactives depuis plus de trois ans.
- ☐ Essayer de faire le tri dans vos bases de données entre les adresses B2B et les adresses B2C, en utilisant un tri par fournisseur de messagerie.
- ☐ Mettre à disposition sur vos sites, au guichet, et par téléphone toutes les mentions légales règlementaires (voir la fiche «Mentions sur vos sites»).
- ☐ Mettre en place un processus de consentement intégralement en règle avec le RGPD (opt-in et opt-out).
- ☐ Enregistrer de façon pérenne la trace des consentements obtenus et des désinscriptions.
- ☐ Instaurer une méthode qui vous permet de savoir la date de votre dernière interaction avec une personne via email.
- ☐ Veiller à n'utiliser les adresses de votre base de données que pour la promotion de votre structure/festival/activité et non celle d'un partenaire, sauf accord spécifique de la personne concernée.
- ☐ Assurer la sécurité et l'accès à votre base de données mail.
- ☐ Mettre à jour votre documentation sur votre protocole de collecte et d'utilisation des adresses mails.

LES COOKIES

Qu'est-ce qu'un cookie ?

Un cookie est un fichier qui est déposé par votre navigateur sur votre ordinateur lorsque vous naviguez sur Internet. Ce fichier est un fichier texte généré par votre site et il est envoyé au navigateur Internet de l'utilisateur de votre site. Ce navigateur va enregistrer le fichier sur le disque dur de l'internaute, votre serveur n'a pas accès directement à son ordinateur. Ils ont différentes finalités telles que :

- La proposition automatique du login et du mot de passe.
- Le stockage des paramètres d'affichage.
- L'analyse des clics et saisies effectués sur le site. Votre site pourra alors proposer en tête de page un spectacle dont le genre est adapté aux précédentes recherches de l'internaute.
- La connaissance des comportements des utilisateurs ; par exemple combien de temps ils restent sur vos pages, comment utilisent-ils les paniers d'achats, etc.
- L'analyse des partages sur les réseaux sociaux.

Les règles des cookies

Les cookies doivent être signalés par un bandeau d'information s'affichant dès la première page et contenant tous les points suivants :

- Les informations sur les finalités d'utilisations des cookies.
- Une demande de consentement qui empêche disparition du bandeau tant que le consentement n'a pas eu lieu.
- Un lien « en savoir plus, vous opposer ou paramétrer vos préférences en matière de cookies » selon le type de cookie (voir ci-dessous).

Sans consentement, il est interdit d'installer des cookies ou de collecter / traiter des données dans l'attente du consentement.

Seul un acte positif constitue un recueil valable du consentement, c'est-à-dire un clic sur un bouton du type « j'accepte » ou « je suis d'accord ».

Même si la CNIL considère que le fait de continuer sa navigation sur le site sur lequel est apparu le bandeau cookie constitue un accord, cette règle pourra être amendée dans le cadre du règlement «e-privacy» aujourd'hui en discussion. Il n'est donc pas recommandé de se fier à ce type de consentement.

Ces bandeaux doivent obligatoirement réapparaitre au bout de **13 mois** pour redemander un consentement et **à chaque fois qu'une nouvelle modalité est ajoutée** aux finalités de traitement.

Deux types de cookies

Les cookies soumis à une simple information « en savoir plus » dans le bandeau :

- Les cookies ayant pour finalité exclusive de permettre ou de faciliter la communication (cookies « identifiant de session » / cookies d'authentification / cookies de personnalisation d'interface)
- Les cookies strictement nécessaires à la fourniture d'un service expressément demandée par l'utilisateur (lecteur multimédia, panier d'achat)
- Certains cookies de mesures d'audience sous certaines conditions

Les cookies soumis à une information « en savoir plus » **et à un consentement** « j'accepte » :

- Les cookies liés aux opérations de publicité ciblée (retargeting).
- Les cookies de mesures d'audience.
- Les cookies traceurs de réseaux sociaux générés par des boutons de partage.

Voir le modèle de mentions pour ces cookies : http://www.droit.co/modèles-de-mentions-pour-les-cookies.html

LES MENTIONS SUR VOS SITES

La présence de **mentions légales** est obligatoire sur votre site, peu importe sa forme ou son contenu. Elles peuvent s'agrémenter d'une **politique de protection des données** si vous collectez de la donnée ; d'une **politique de cookies** si vous en utilisez ; et enfin de **conditions générales de vente** pour la vente en ligne.

Ces informations garantissent un certain niveau de transparence en offrant aux internautes la possibilité de vérifier l'identité de l'éditeur et le fonctionnement des traitements de données.

Ces mentions sont toutes sous la responsabilité du responsable de traitement.

Le sous-traitant peut aider à leur rédaction si besoin sur des sujet de technologie ou de sécurité, mais le responsable de traitement étant décisionnaire de la finalité des traitements de données, il lui revient d'en décider du contenu.

D'autres mentions sont ajoutables selon vos besoins comme détaillées ci-dessous :

Les mentions légales

Ces mentions doivent apparaitre obligatoirement sur tous les sites.

- La raison sociale, forme juridique, adresse de l'établissement ou du siège social (et non pas une simple boîte postale), montant du capital social ;
- Nom adresse et contact de l'hébergeur du site.
- Nom du directeur de la publication.
- L'adresse de courrier électronique et numéro de téléphone ;
- Pour une activité commerciale : numéro d'inscription au registre du commerce et des sociétés (RCS) ;
- En cas d'activité commerciale : numéro individuel d'identification fiscale numéro de TVA intracommunautaire ;
- Pour une profession réglementée : référence aux règles professionnelles applicables et au titre professionnel ;
- Nom et adresse de l'autorité ayant délivré l'autorisation d'exercer quand celle-ci est nécessaire.

La politique de confidentialité

Cette mention doit apparaitre obligatoirement sur votre site si vous collectez de la donnée.

- L'identité et les coordonnées du **responsable du traitement** (ou du représentant du responsable du traitement).
- L'identité et les coordonnées de contact du « **Data Protection Officer** » si ce poste existe dans votre structure.
- Les **finalités du traitement** ainsi que la base légale qui prouve que vous avez le droit de traiter les données (consentement explicite du visiteur, obligations légales…).
- Les **destinataires** ou les catégories de destinataires des données à caractère personnel.
- Le transfert éventuel de données vers une autre organisation ou un pays tiers.
- La **durée de rétention des données** et les critères qui déterminent cette durée. Par exemple combien de temps gardez-vous les données des soumissions de votre formulaire de contact ?
- Le droit du visiteur de demander **l'accès à ses données** à caractère personnel détenues par le responsable du traitement, mais également le droit de rectification, modification ou effacement. La personne concernée a également le droit de demander que le traitement qui la concerne soit limité, ou de s'opposer au traitement de ses données.
- Le droit du visiteur à demander une **copie des données** dans un format structuré (Droit à la portabilité).
- Le droit d'introduire une réclamation auprès d'une autorité de la **CNIL**. Les informations utiles concernant un **éventuel profilage** ainsi que les conséquences pour la personne concernée.

L'utilisation de cookies

Cette mention doit apparaitre sur votre site si vous utilisez des cookies.

- Le nom technique du cookie.
- La durée de conservation.
- La finalité.
- Le fonctionnement (dans les grandes lignes).
- Le statut juridique qui vous autorise à utiliser ce cookie.

L'utilisation d'outils de tracking

Si vous utilisez des outils de tracking tels que Google Analytics ou Hotjar pour analyser le trafic de votre site Web et le comportement des utilisateurs, vous devez également mentionner pour chaque outil : le nom, les données collectées, la finalité du traitement et la période de rétention des données.

Il est également important de donner au visiteur la possibilité de refuser le suivi de sa visite à des fins statistiques. Il peut ainsi suivre les procédures d'opt-out généralement disponibles pour ce type d'outil.

Les conditions générales de ventes

Ces conditions doivent apparaitre sur votre site si vous vendez des produits ou des services en ligne, mais elles ne sont pas directement liées au RGPD, nous n'aborderons donc pas leurs contenus ici.

La propriété intellectuelle

Cette mention n'est pas obligatoire mais peut préciser que les éléménts du site internet sont la propriété intellectuelle de l'éditeur du site et qui ne peuvent en aucun cas être repris, complétement ou partiellement, sans autorisation.

Disclaimer

Cette mention a pour but de **décliner ou limiter les responsabilités de l'éditeur du site**, par exemple en ce qui concerne la véracité ou l'exactitude des informations proposées sur votre site, ou encore la validité des liens hypertextes proposés.

FAILLE DE SÉCURITÉ

Dans le domaine de la sécurité informatique, une vulnérabilité ou faille est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système. C'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Pour vous aider à évaluer le niveau de sécurité de votre structure, retrouvez la checklist de la CNIL dans notre boîte à outils > Évaluation du niveau de sécurité des données personnelles de votre structure.

Comment réagir face à une faille de sécurité ?

1. Identifier et corriger le problème à l'origine de la faille.
2. La faille doit être signalée à la hiérarchie > DPO > sous-traitant ou responsable de traitement.
3. Constituer un dossier de preuves pour documenter la prise en charge de cette faille (contrôle de l'origine de la faille, responsabilités, audits de sécurité, tests et routines de sécurité, etc.).
4. Déposer une plainte ainsi qu'une déclaration aux assurances.
5. Notifier la faille à la CNIL dans les 72 heures sauf dans les cas détaillés ci-dessous.
   Voir boîte à outils > Dossier CNIL «Notification de violation de données à caractère personnel»
6. Communiquer aux personnes concernées par la violation de leurs données si besoin est.
7. Documenter la prise en charge de la faille et les mesures prises pour y remédier et l'éviter.

Notification à la CNIL (Art 33)

La notification à l'autorité de contrôle d'une violation de données doit être faite dans les 72 heures à partir du moment où ils en ont connaissance. Elle doit contenir :

- Une description de la nature de la violation,
- les coordonnées du DPO ou du contact,
- les conséquences probables de la violation,
- les mesures prises pour remédier à la violation,
- une documentation de l'incident.

Notification à la personne concernée par une violation de données (Art 34)

- Si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, la communication doit être effectuée dans le plus brefs délais.
- Le contenu de cette notification doit être prédéfinie et avoir été pensé avant qu'un incident ne survienne en utilisant un langage clair et simple.
- La communication à la personne concernée n'est pas nécessaire si :
  - » S'il y a preuve de la mise en œuvre des mesures de protection techniques et organisationnelles appropriées et que ces mesures ont été appliquées aux données.
  - » Le risque élevé pour les droits et les libertés des personnes concernées n'est plus susceptible de se matérialiser.
  - » Cette communication exigerait des efforts disproportionnés par rapport à la gravité de la violation.

LES SOUS-TRAITANTS

Bien qu'il ne soit pas « responsable du traitement », le sous-traitant traite des données pour le compte d'un autre organisme dans le cadre d'un service ou d'une prestation (exemple : un prestataire de billetterie fait des opérations de prospection par mail pour le compte d'un théâtre).

A ce titre, le sous-traitant est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et de documentation de leur activité. Le responsable de traitement reste néanmoins celui qui « détermine les finalités et les moyens d'un traitement » (art.4), c'est-à-dire la structure qui sollicite la prestation.

1. Obligation de transparence et de traçabilité

Le sous-traitant doit :

- Établir un contrat ou une clause aux contrats existants précisant les obligations de chaque partie (art 28.)
- Recenser par écrit les instructions des clients concernant les traitements de données.
- Demander l'autorisation écrite du client si le sous-traitant fait appel à un sous-traitant lui-même.
- Mettre à disposition de ses clients toutes les informations nécessaires pour démontrer le respect de ses obligations et permettre la réalisation d'audit.
- Tenir un registre qui recense ses clients et décrit les traitements effectués pour leurs comptes.

2. Obligation de protection des données dès la conception et par défaut

Le sous-traitant doit offrir à ses clients les garanties nécessaires pour que le traitement soit en conformité avec le RGPD.

- Dès la conception des outils, produits, applications ou services
- Par défaut, c'est-à-dire que seules les données nécessaires à la finalité du traitement sont traitées, et ce au regard de la quantité de données collectées, de l'étendue de leur traitement, de la durée de conservation, et du nombre de personnes qui y ont accès.

3. Obligation de garantie de protection de la donnée

- Les employés du sous-traitant doivent être soumis à une obligation de confidentialité.
- Toute violation doit être notifiée aux clients dans de brefs délais.
- Des mesures doivent garantir un niveau de sécurité adapté aux risques.
- Au terme de la prestation, le sous-traitant doit, en accord avec le client, supprimer toutes les données ou les renvoyer au client et en détruire les copies existantes sauf si obligation légale de les conserver.

4. Obligation d'assistance et conseil

Le sous-traitant se doit d'aider ses clients à se mettre en conformité avec le RGPD en les aidants dans leurs réalisations d'impact sur la vie privée, en les notifiant en cas de violation de données, en les conseillant sur des mesures de sécurité, en les aidant lorsqu'une personne exerce ses droits d'accès ou de rectification, en les alertant si leurs instructions sont contraires au RGPD.

Les contrats de sous-traitance

Le contrat de sous-traitance doit définir :

- L'objet et la durée de la prestation
- La nature et la finalité du traitement
- Le type de données à caractère personnel traitées
- Les catégories de personnes concernées
- Les obligations et les droits de vos clients, en tant que responsable de traitement
- Les obligations et les droits du sous-traitant tels que prévus par l'article 28.

Les contrats de sous-traitance

Tous les contrats de sous-traitance en cours d'exécution devront être agrémentés des clauses obligatoires prévues par le RGPD.

Voir l'exemple de clauses à la page 13 du Guide du sous-traitant de la CNIL

Le registre obligatoire de traitement du sous-traitant doit contenir :

- Le nom et les coordonnées de chaque client pour le compte duquel vous traitez des données.
- Le nom et les coordonnées de chaque sous-traitant ultérieur
- Le nom et les coordonnées du délégué à la protection des données
- Les catégories de traitement effectuées pour le compte du client
- Les transferts de données hors UE
- Une description générale des mesures de sécurité techniques et organisationnelles déployées.

Modèle de registre de la CNIL

https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx

BOÎTE À OUTILS

REGLEMENT GENERAL SUR LA PROTECTION DES DONNES

http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679

DOSSIER CNIL « SE PRÉPARER EN 6 ÉTAPES »

https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf

DOSSIER CNIL « GUIDE DU SOUS-TRAITANT »

https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

DOSSIER CNIL « LA SÉCURITÉ DES DONNÉES PERSONNELLES »

https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

DOSSIER CNIL « LIGNES DIRECTRICES CONCERNANT L'ANALYSE D'IMPACT »

https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

DOSSIER CNIL « RÉFÉRENTIEL DE DURÉE DE CONSERVATION DES DONNÉES »

https://www.cnil.fr/sites/default/files/typo/document/20120719-REF-DUREE_CONSERVATION-VD.pdf

DOSSIER CNIL « QUE FAIRE QUAND VOTRE ENTREPRISE COMMUNIQUE ET/OU VEND EN LIGNE »

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_fiche-1_que-faire-quand-votre-entreprise-communique-vend-en-ligne.pdf

DOSSIER CNIL & BPI « GUIDE PRATIQUE DE SENSIBILISATION AU RGPD DES PME »

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf

DOSSIER CNIL « NOTIFICATION DE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL »

Notice

https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Formulaire téléchargeable

https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf

Outil d'auto-évaluation de violation de données personnelles

https://www.cnil.fr/sites/default/files/typo/document/Notifications-AutoEvaluation.xls

MODÈLES DE MENTIONS CNIL

Panneau d'information « Établissement sous surveillance »

https://www.cnil.fr/fr/modele/mention/panneau-dinformation-video-surveillance

Dispositif d'accès par badge

https://www.cnil.fr/fr/modele/mention/dispositif-dacces-par-bagdes

Formulaire de collecte de données personnelles

https://www.cnil.fr/fr/modele/mention/formulaire-de-collecte-de-donnees-personnelles

Enregistrement de conversations téléphoniques

https://www.cnil.fr/fr/modele/mention/enregistrement-de-conversations-telephoniques

Notice d'information en matière de recrutement

https://www.cnil.fr/fr/modele/mention/notice-dinformation-en-matiere-de-recrutement-0

MODÈLE DE MENTIONS LÉGALES D'UN SITE WEB

https://www.service-public.fr/professionnels-entreprises/vosdroits/F31228

GÉNÉRATEUR DE MENTIONS LÉGALES D'UN SITE WEB

https://www.donneespersonnelles.fr/mentions-legales-site-internet

https://generateur-de-mentions-legales.com

MODÈLE DE MENTIONS POUR LES COOKIES

http://www.droit.co/modèles-de-mentions-pour-les-cookies.html

MODÈLES DE REGISTRE

Dernier modèle proposé par la CNIL (en mai 2018) et ayant vocation à être plus simple à utiliser :
https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

Autres modèles de registre :
https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx

EVALUATION DU NIVEAU DE SECURITÉ DES DONNÉES PERSONELLES DE VOTRE STRUCTURE

https://www.cnil.fr/sites/default/files/atoms/files/check_list_0.pdf

SOURCES

http://www.droit.co/mod%C3%A8les-de-mentions-pour-les-cookies.html

https://blog.defimedia.be/expertise/les-mentions-legales-de-votre-site-web-sont-elles-correctes/

https://iconewsblog.org.uk/2018/05/09/raising-the-bar-consent-under-the-gdpr/

https://www.avocat-rgpd.com/single-post/2017/12/19/RGPD-Comment-archiver-les-donn%C3%A9es-personnelles-

https://www.cnil.fr/

https://www.cnil.fr/cnil-direct/attachement/514/92

https://www.cnil.fr/fr/cnil-direct/question/845

https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi

https://www.cnil.fr/fr/designation-dpo

https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee

https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants

https://www.cnil.fr/fr/rgpd-en-pratique-maitrisez-votre-relation-client

https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique

https://www.cnil.fr/fr/site-web-cookies-et-autres-traceurs

https://www.culture-informatique.net/cest-quoi-hachage/

https://www.culture-informatique.net/cest-quoi-les-cookies/

https://www.dpms.eu/dpo/choisir%E2%80%8B-%E2%80%8Bun%E2%80%8B-%E2%80%8Bdelegue%E2%80%8B-%E2%80%8Bprotection%E2%80%8B-%E2%80%8Bdonnees/

SOURCES

https://www.journaldunet.fr/business/dictionnaire-economique-et-financier/1199121-b-to-b-ou-b2b-definition-traduction/

https://www.lemagit.fr/conseil/Droit-a-loubli-et-RGPD-anonymisation-ou-suppression-des-donnees-un-choix-difficile

https://www.lemagit.fr/definition/Hachage

https://www.service-public.fr/professionnels-entreprises/vosdroits/F31228

https://www.solutions-numeriques.com/fichiers-clients-et-prospects-quelle-duree-de-conservation-avec-la-nouvelle-norme-ns-48/

https://www.theguardian.com/technology/2018/may/21/gdpr-emails-mostly-unnecessary-and-in-some-cases-illegal-say-experts

Directrice de publication : Olivia Vergnon
Design et mise en page : Guillaume Nadjar - www.omidesign.net

EntreeDirecte - Juin 2018

ENTREEDIRECTE.FR

moteur de tous vos spectacles

EntreeDirecte.fr c'est la startup indépendante qui redonne la part belle à ceux qui font vraiment le spectacle vivant partout en France.

ED c'est le moteur de recherche qui met tous les spectacles sur un pied d'égalité et vous reconnecte à votre public.

ED c'est un projet ambitieux qui fait la lumière sur notre diversité culturelle par l'intelligence de la data.

ED c'est la proposition simple et rapide qui regroupe tous les outils dont vous avez besoin.

Consacrez-vous à l'essentiel :

faire vivre le spectacle vivant
partout, par tous et pour tous.

contact@entreedirecte.fr
corporate.entreedirecte.fr | www.entreedirecte.fr

#spectaclepartout **#spectaclepartous** **#spectaclepourtous**