GHR
GROUPEMENT DES HOTELLERIES
& RESTAURATIONS DE FRANCE

Guide RGPD 2023

Mise en place de la protection des données

Groupement national des indépendants
Hôtellerie & Restauration

Table des matières

Présentation des obligations relatives à la protection des données

Le Règlement général sur la protection des données est entré en vigueur le 25 mai 2018 (Lire ici notre article sur le contenu de ce Règlement). La loi française relative à la protection des données a été publiée le 20 juin 2018 et vient notamment poser les nouvelles compétences de la CNIL. Pour vous accompagner le GHR vous donne ses conseils adaptés au secteur de l'hôtellerie-restauration **pour vous accompagner dans la protection des données personnelles collectées**.

A noter dès à présent

- ✓ **Toutes les données personnelles sont concernées** : celles des salariés, des clients, des prospects et des fournisseurs.
- ✓ **Il n'y a plus de déclaration préalable** à effectuer auprès de la CNIL (Ex : vidéosurveillance, fichiers de candidats…).
- ✓ Un établissement du secteur HCR, du fait de son activité, n'a **pas l'obligation de désigner un Délégué à la Protection des données**.
- ✓ **Tous les supports (numérique et papier) sont concernés** par le Règlement.
- ✓ Tous les documents et toutes les procédures relatives à la protection des données sont **à conserver au même endroit** pour les présenter facilement en cas d'un éventuel contrôle.

Le renforcement des droits des individus

Les personnes dont les données ont été collectées ont le droit :

- de **rectifier** leurs données si celles-ci sont inexactes,
- de demander la **suppression** des données, si elles ne sont plus nécessaires à la finalité de la collecte et dans la limite des durées légales,
- de **limiter le traitement** des données,
- **de recevoir les données dans un format couramment utilisé et lisibles par machine,**
- de **s'opposer à un traitement** de données, notamment en cas de prospection ou de profilage.

Les obligations des entreprises

Le RGPD repose essentiellement sur une obligation majeure : **la responsabilisation de chaque acteur à chaque étape de gestion des données personnelles**.

Envers chaque individu dont les données personnelles sont collectées, les entreprises du secteur doivent :

- **Communiquer sur les finalités** de la collecte des données.
- **Obtenir le consentement** des personnes dont les données sont collectées. Cela est notamment très fortement conseillé avant tout marketing direct envers les anciens clients.
- Donner aux clients **accès à leurs données**, notamment pour leur permettre de les envoyer à d'autres entreprises (Droit à la portabilité).
- **En cas de problème de sécurité des données** représentent un risque élevé pour les droits et libertés des personnes, celles-ci doivent en **être informées.**
- **Supprimer les données à la fin de la durée légale de conservation et/ou sur demande expresse.**
- Permettre aux personnes de **s'opposer au traitement en vue de marketing direct**.

Les entreprises doivent également faire le point sur l'ensemble des données personnelles qui sont collectées en remplissant leur Registre (voir ici les modèles CNIL). En faisant cela, chaque établissement sera en mesure d'améliorer ses procédures internes de protection des données (respect des durées de conservation, cybersécurité…)

Les actions à mener

<table>
<tr><th></th><th>Employés</th><th>Clients</th><th>Fournisseurs</th><th>Sous-traitants</th></tr>
<tr><td>1</td><td colspan="4">Déterminer la personne référente aux données personnelles dans l'entreprise.
Les entreprises du secteur HCR, du fait de leur activité, n'ont pas l'obligation de désigner un Délégué à la Protection des données (DPO) Néanmoins la CNIL recommande d'avoir une personne qui centralise toutes les informations, notamment en contact pour les salariés (anciennement le Correspondant Informatique et Liberté). Par défaut il s'agira donc du chef d'entreprise.
Lien pour désigner un DPO à la CNIL.</td></tr>
<tr><td rowspan="3">2</td><td colspan="4">Informer tous les individus pour lesquels les données personnelles sont collectées et traitées.</td></tr>
<tr><td>Information dans le contrat de travail/l'avenant aux contrats de travail, le Règlement intérieur, Note interne (voir modèles GHR)</td><td>Mail d'information aux anciens clients (voir modèle GHR)</td><td>Mail d'information aux fournisseurs (voir modèle GHR)</td><td>Mail demandant la signature des nouvelles clauses de partage de responsabilité (voir modèle GHR)</td></tr>
<tr><td>Information des candidats en cas de conservation des données personnelles contenues dans les CV (Voir modèle GHR).</td><td>Modification des conditions générales de vente avec les clauses de respect de la protection des données (voir modèle GHR)
Demande de consentement pour tout usage des données ne relevant pas du contrat de prestation (ex: mails marketing) (voir modèle GHR)</td><td></td><td>Conservation de tous les avenants/nouveaux contrats prenant en compte les obligations du RGPD</td></tr>
<tr><td>3</td><td colspan="4">Réaliser son registre de protection des données
Pour les plus de 250 employés :
https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx
Pour les moins de 250 salariés :
https://www.cnil.fr/sites/cnil/files/atoms/files/registre_rgpd_basique.pdf</td></tr>
<tr><td>4</td><td colspan="4">Mise en place des mesures de sécurité des données dès la conception des systèmes informatiques et mise en place de procédures internes et d'information des collaborateurs en charge de traitement de tout ou partie des données personnelles (Voir les Conseils en cybersécurité)</td></tr>
<tr><td>5</td><td colspan="4">Suppression des données
• lorsque demandé par la personne (dans la limite des durées légales)
• à l'expiration des durées légales
• à l'expiration des durées fixées par l'entreprise</td></tr>
<tr><td>6</td><td colspan="4">Informer les individus en cas de problème de sécurité des données représentant un risque élevé pour leurs droits et libertés (voir modèle GHR).</td></tr>
</table>

Chaque établissement doit ainsi détenir un dossier de conformité à présenter en totalité ou en partie sur demande de la CNIL ou des individus concernés. Il doit contenir :

- Le registre de protection des données (Voir le Chapitre dédié) ;
- Les modèles de mentions d'information (Voir le Chapitre dédié) ;
- Les contrats des sous-traitants (Voir le Chapitre dédié) ;
- Le recueil de consentement ;
- Les violations subies et les mesures de sécurité appliquées (Voir le Chapitre dédié);
- Les documents internes de sensibilisation, les procédures à suivre…

Liste des durées légales de conservation

Les données doivent être supprimées après l'extinction de la durée légale de conservation. Il y a une tolérance sur les données qui peuvent faire l'objet de contentieux, de sortes à pouvoir les conserver jusqu'à l'épuisement des délais de recours en justice.

Il est également possible d'archiver, plutôt que de supprimer, mais les objectifs devront être clairement explicités. De même la durée d'archivage et la sécurité de ces données archivées devront être précisées. Il est recommandé d'archiver sur des serveurs distincts des serveurs stockant les données « actives », avec un accès très limité à ce serveur, voire idéalement sur des machines non connectées au web.

Si l'établissement n'est pas en mesure techniquement d'assurer une suppression au jour le jour des données, il est recommandé d'avoir une tâche récurrente pluriannuelle (selon la taille de l'établissement et des données collectées), tous les 3 ou 6 mois, au début et à la fin de chaque saison pour les établissements saisonniers.

Les données des fournisseurs

Type de document	**Durée de conservation**	**Texte de référence**
Contrat ou convention conclu dans le cadre d'une relation commerciale, correspondance commerciale	5 ans	Article L110-4 du code de commerce
Contrat conclu par voie électronique (à partir de 120 €)	10 ans à partir de la livraison ou de la prestation	Article L213- 1 du code de la consommation
Document bancaire (talon de chèque, relevé bancaire...)	5 ans	Article L110-4 du code de commerce
Document de transport de marchandises	5 ans	Article L110-4 du code de commerce
Dossier d'un avocat	5 ans à partir de la fin du mandat	Article 2225 du code civil
Pièce justificative : bon de commande, de livraison ou de réception, facture fournisseur, etc.	10 ans à partir de la clôture de l'exercice	Article L123-22 du code de commerce

Les données des employés

Type de document	Durée de conservation	Texte de référence
Bulletin de paie	5 ans	Article L.3243-4 du code du travail
Registre unique du personnel	5 ans à partir du départ du salarié	Article R.1221-26 du code du travail
Documents concernant les contrats de travail, et la rémunération (salaires, primes, indemnités, soldes de tout compte, régimes de retraite, etc…)	5 ans	Article 2224 du code civil
Documents relatifs aux charges sociales et à la taxe sur les salaires	3 ans	Article L.244-3 du code de la sécurité sociale et art. L.169 A du livre des procédures fiscales
Comptabilisation des jours de travail des salariés sous convention de forfait	3 ans	Article D.3171-16 du code du travail
Comptabilisation des horaires des salariés, des heures d'astreinte et de leur compensation	1 an	Article. D.3171-16 du code du travail
Observation ou mise en demeure de l'inspection du travail Vérifications et contrôles et mis à la charge de l'employeur au titre de la santé et de la sécurité au travail	5 ans	Article D.4711-3 du code du travail
Déclaration d'accident du travail auprès de la caisse primaire d'assurance maladie	5 ans mais il est conseillé de conserver tous les documents liés aux accidents du travail pendant un délai de 10 ans, au terme duquel l'action en responsabilité de la victime est prescrite	Article D.4711-3 du code du travail Article 2226 du Code civil
Données individuelles du salarié (contrat de travail, convocation à un entretien préalable, lettre de licenciement, dossier disciplinaire…)	Il est conseillé de les conserver pendant au minimum 2 ans pour prévenir d'un éventuel litige prudhommal (contestation licenciement par exemple)	Article L.1471-1 du code du travail
Données issues des badges d'accès du personnel	3 mois	Recommandation CNIL

Les données des clients

Données collectées si nécessaire et selon l'activité de l'établissement.

Type de document	**Durée de conservation**	**Texte de référence**
Informations liées à la réservation d'un client	3 ans à compter de la fin de la relation commerciale	CNIL
Contrat ou convention conclu dans le cadre d'une relation commerciale, correspondance commerciale	5 ans	Article L110-4 du code de commerce
Garantie pour les biens ou services fournis au consommateur	2 ans	Article L218-2 du code de la consommation
Contrat conclu par voie électronique (à partir de 120 €)	10 ans à partir de la livraison ou de la prestation	Article L213- 1 du code de la consommation
Pièce justificative : facture client, etc.	10 ans à partir de la clôture de l'exercice	Article L123-22 du code de commerce
Prospects	3 ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect	CNIL
Pièces d'identité	Il n'est pas possible de collecter les copies des pièces d'identité.	CNIL
Cartes bancaires	Le temps de la transaction financière (paiement effectif)	Article L. 221-18 du code de la consommation
	13 mois après la date de débit (en archive intermédiaire et uniquement le numéro et la date de validité pour constituer une preuve en cas de contestation de la transaction)	Article L. 133-24 du code monétaire et financier
	Plus longtemps avec l'autorisation explicite du client (en cas de paiement régulier par exemple)	
Statistiques de mesure d'audience (Ex : Cookies)	13 mois	
Données issues des badges d'accès des clients	3 mois	Recommandation CNIL

Registre de protection des données

La CNIL a publié deux modèles de registre de protection des données. Le GHR vous livre ses conseils pour les remplir.

Pour les entreprises de moins de 250 salariés

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

1. **Responsable de traitement des données** : Par défaut, le responsable de la structure de moins de 250 salariés est le responsable de la protection des données. Il est néanmoins possible de déléguer cette activité à une autre personne (DRH, Directeur juridique…). Le contact de cette personne sera donc à signaler dans les documents d'information à destination des salariés, des clients et des fournisseurs. Il est alors recommandé de remplir deux cases : une pour le responsable légal et une pour le responsable à la protection des données, sans forcément la désigner comme DPO.
2. **Liste des traitements** : Considérer dans un premier temps chaque catégorie de cible (employés, clients, fournisseurs) et répertorier toutes les procédures qui nécessitent l'usage de données personnelles (dès l'utilisation du nom de famille ou d'une coordonnée notamment)

Pour les salariés il s'agira (liste non exhaustive) : recrutement, embauche (contrat de travail, registre unique du personnel…), bulletin de paie…

Pour les clients il s'agira (liste non exhaustive) : le contrat de prestation, les documents de facturation, les données bancaires…

A noter que chaque sous-traitant ou prestataire peut également posséder des données personnelles concernant les employés ou les clients. Il est donc nécessaire de répertorier ici aussi toutes les procédures de gestion de données traitées en externe (bulletin de paie, CRM…)

3. **Fiche d'activité** : Une fiche est à remplir pour chaque ligne du tableau précédent.

Le nom du responsable conjoint du traitement est le nom de la personne qui gère cette activité. Par exemple pour le bulletin de paie, il peut s'agir du Directeur/-trice du personnel, du Directeur/-trice du service comptabilité, du responsable chez un prestataire…

Objectifs poursuivis : la description doit signaler les différentes étapes de l'activité pour lesquelles les données sont utilisées. Ex pour la gestion CRM : La collecte des données est effectuée lors de la réservation de la prestation hôtelière/de restauration, le mailing est conçu en fonction des consommations antérieures de ce client, un lien de désinscription est toujours disponible en bas de chaque email, un suivi statistique est effectué pour chaque ouverture et clic dans un mail…

Durées de conservation des catégories de données : Se reporter à la partie concernée de ce document. Préciser s'il s'agit d'une durée légale ; dans le cas contraire, préciser le document où se trouve l'information pour la personne concernée.

Transferts des données hors UE : Se renseigner auprès des sous-traitants sur les pays où se trouvent leurs serveurs informatiques (notamment pour les prestataires internationaux : Booking.com, Expedia, La Fourchette…)

Mesures de sécurité : Ne pas hésiter le cas échéant de préciser les modalités pratiques organisationnelles du type formation à la cybersécurité des salariés, rappel des règles informatiques dans une Charte informatique annexée au Règlement intérieur (modèle GHR disponible sur demande) …

Pour les entreprises de plus de 250 salariés

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

Onglet « Liste des traitements »

Ce modèle de document fourni par la CNIL permet à l'entreprise d'établir une nomenclature des traitements des données pour faciliter la cartographie de l'usage des données personnelles. Le GHR recommande aux entreprises du secteur HCR concernés de procéder à un référencement des traitements, par établissement (HOT/REST/BRAS/TRAIT… et numéro simple ou code postal), par catégorie de personnes concernées (Employés/clients/prospects/fournisseurs), par service/sous-traitant (Compta/Commerc/Commun/CRM/Nom du prestataire…) concerné puis enfin une numérotation par importance des traitements. Le GHR recommande aussi de créer un onglet spécifique pour l'explication de la nomenclature. Ex : REST-EMPL-COMPTA-001 ou HOT75002-CL-CRM-001

Onglet « Modèle fiche registre »

Cet onglet est à dupliquer pour chaque ligne du tableau de l'onglet précédent recensant la liste des traitements. Pour des facilités de consultation et éviter la perte de l'intégralité du document, le GHR recommande aux entreprises possédant plusieurs établissements de concevoir plusieurs documents :

- un document de nomenclature avec TOUS les traitements de l'entreprise,
- un document avec les traitements gérés au niveau du siège,
- un document par établissement.

Selon la taille de chaque établissement, il peut être nécessaire de sous-diviser encore les documents.

Pour concevoir ce registre, il est possible que chaque collaborateur impliqué (chef d'établissement, directeur des départements internes…) aide à sa conception même si une personne désignée référente doit veiller à la bonne homogénéisation de l'ensemble du document.

Nom du traitement : Désignation de l'activité de traitement sans détail.
Responsable du traitement : Personne en charge de cette activité. Ex : DRH pour l'activité embauche ; un Sous-traitant pour la gestion du CRM
Responsable(s) conjoint(s) : Collaborateurs qui ont une responsabilité en lien avec ce traitement. Il peut s'agir d'un sous-traitant ou à l'inverse du collaborateur en charge du sous-traitant ayant la responsabilité du traitement.

Finalités du traitement : Indiquer ici le détail du traitement. Ex : pour le traitement embauche la finalité principale est la rédaction du contrat de travail, la sous-finalité 1 peut être le Registre unique du personnel, la sous-finalité 2 peut être la conception de l'organigramme…

Mesures de sécurité techniques :

- Contrôle d'accès des utilisateurs
- Mesures de traçabilité
- Mesures de protection des logiciels
- Sauvegarde des données
- Chiffrement des données

Mesures de sécurité organisationnelles :

- Contrôle des sous-traitants,
- Sensibilisation des collaborateurs par des formations régulières,
- Charte informatique en annexe du Règlement intérieur (modèle disponible sur demande au GHR)

Catégories de données personnelles concernées : le liste des types de données personnelles concernées sont à remplir dans la case description.

Délai d'effacement : Le GHR recommande de préciser si ce délai reprend un délai légal ou non (Se reporter à la partie concernée de ce document) S'il ne s'agit pas d'une durée légale, il peut être précisé le nom du document où l'individu peut connaître la durée de conservation (Ex : Conditions générales de Vente pour une réservation hôtelière)

Catégories de personnes concernées : Préciser la catégorie de personne concernée (Employé, client, prospect, fournisseurs)

Destinataires : Il s'agit ici de préciser les collaborateurs concernés en interne, des organismes externes de type siège social/filiale ou partenaires (conventionnés), et les sous-traitants/prestataires.

Transferts hors UE : Si l'entreprise a un siège ou à l'inverse une filiale en dehors de l'UE, il est nécessaire de le préciser ici.
Le GHR recommande de s'assurer auprès des prestataires et sous-traitants avant tout extra-européens, où se situent leurs serveurs informatiques de conservation et traitement.

Les FAQ du RGPD

Identifier les données personnelles

1. Qu'est-ce qu'une donnée personnelle ?

La CNIL donne pour définition : « Toute information identifiant directement ou indirectement une personne physique (ex. nom, no d'immatriculation, no de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...). »

2. Est-ce que les données fournisseurs sont concernées par le RGPD ?

A partir du moment où un fournisseur vous a communiqué des données personnelles comme contact, alors ces données sont concernées par le RGPD.

L'entreprise doit donc recenser auprès du service comptabilité tous les fournisseurs et auprès de tous les collaborateurs, toutes les données personnelles collectées.

3. Est-ce que les données contenues dans mes archives papier sont concernées ?

Oui. Le Règlement européen ne précise jamais le support contenant les données personnelles. Par ailleurs la Loi française relative à protection des données personnelles précise que la CNIL a la compétence pour demander les documents nécessaires « quel qu'en soit le support ».

Les obligations des établissements CHR

4. Je suis un établissement CHR de plus de 250 salariés, dois-je avoir un Délégué à la Protection des données ?

Non, le Délégué à la Protection des données (DPO) n'est pas obligatoire pour un établissement du secteur CHR compte tenu de l'activité menée et du type de données collectées. Néanmoins une personne doit être indiquée comme responsable de la protection des données. Il s'agira du chef d'entreprise par défaut si personne d'autre n'est signalé.

5. Je suis un établissement CHR de moins de 250 salariés, dois-je tenir un Registre des données personnelles ?

Le Règlement européen n'impose pas de Registre des données personnelles aux TPE-PME. Néanmoins la CNIL qui a la compétence pour effectuer les contrôles, demande à ce qu'un registre soit disponible également dans les TPE-PME françaises. Voir ici le modèle et les conseils pour le remplir.

6. Je suis un établissement CHR quel peut être le type de données sensibles que je collecte ?

Les données sensibles qui peuvent être collectées par les établissements du secteur CHR sont :

- S'agissant des employés : des coordonnées, des informations de santé, des informations syndicales…
- S'agissant des clients : des cartes bancaires, des pièces d'identité, des informations de santé…

7. Je suis un établissement CHR, dois-je procéder à une analyse d'impact ?

Non les établissements CHR ne gèrent pas des données à fort risque pour les droits et libertés des individus. Dès lors, l'analyse d'impact n'est pas rendue obligatoire par le texte européen. Néanmoins il est recommandé de faire une auto-évaluation de la conformité à l'ensemble des obligations.

Le consentement

8. Pour faire une embauche je collecte des données personnelles, comment obtenir le consentement de l'individu ?

La collecte des informations personnelles effectuée dans le cadre d'un contrat, tel un contrat de travail, est considérée comme une collecte ayant obtenu de fait le consentement de l'autre partie au contrat (ici le nouvel employé).

9. Pour faire une réservation je collecte des données personnelles, comment obtenir le consentement de l'individu ?

La collecte des informations personnelles effectuée dans le cadre d'un contrat, tel un contrat de prestation, est considérée comme une collecte ayant obtenu de fait le consentement de l'autre partie au contrat (ici le client). En revanche si les données collectées au moment de la réservation serviront à des fins marketing ou à des activités autres que la prestation hôtelière/de restauration, alors le client devra être clairement informé de l'usage qui sera fait de ses données. Voir ici le modèle de clause dans les Conditions générales de vente.

10. Comment obtenir le consentement des individus pour leur envoyer des communications marketing lorsque les données sont collectées à l'oral (à l'accueil par exemple) ?

Si les données sont collectées à l'oral, le client ne doit pas ignorer les Conditions générales de vente (voir la question ci-dessus). Néanmoins un rappel de l'usage qui sera fait des données peut être fait également à l'oral.

11. Comment obtenir le consentement des individus pour lesquels j'ai collecté les données personnelles avant l'entrée en vigueur de ces obligations ?

Il n'est pas obligatoire de revenir sur le consentement d'une collecte de données effectuée avant l'entrée en vigueur du Règlement européen. Néanmoins, dans un souci d'information aux clients, le GHR a rédigé un modèle de mail qui peut être utilisé pour prévenir de leurs nouveaux droits les anciens clients d'un établissement dont les données sont conservées, notamment à des fins marketing. Voir ici le modèle de mail aux anciens clients.

La suppression des données

12. Dois-je supprimer les données sur mon Registre unique du personnel papier ?

Le Règlement européen exige en effet que l'entreprise ne conserve pas de données, quel qu'en soit le support, au-delà du délai nécessaire, notamment des durées légales. Voir ici les durées légales de conservation des données sociales.

Néanmoins, cette règle était valable précédemment et des inspecteurs du travail ont pu, ponctuellement reprocher à l'entreprise la suppression des lignes sur le Registre unique du personnel en format papier. Le GHR recommande donc dans les premiers temps de l'application du RGPD de ne pas modifier les versions papier (Ex : Registre unique du personnel)

13. Dois-je supprimer les bulletins de salaire de mes salariés ?

Selon l'Article L.3243-4 du code du travail, le bulletin de paie doit être conservé 5 ans par l'employeur (Voir ici les durées légales de conservation) L'usage de conserver à vie ces bulletins n'est pas légal. Il est cependant possible de spécifier dans le Registre de protection des données personnelles que les bulletins seront archivés à partir de 5 ans, sur un serveur spécifique, en indiquant que la durée de conservation sera de 5 ans après le départ du salarié de l'entreprise dans l'objectif d'accompagner les salariés dans la conservation de documents fondamentaux pour le calcul de leurs droits (retraite, chômage, contrôle fiscal…) sur le principe de faveur.

La cybersécurité dans un établissement HCR

La cybersécurité d'un établissement HCR n'est pas à négliger car c'est un secteur qui subit un grand nombre d'attaques (11 attaques fructueuses par an sur 12 menées). Par ailleurs en cas de vol de données personnelles (Lire ici les actions à mener), l'établissement doit avertir tous ses clients qui ont été potentiellement concernés (Lire ici le modèle de courrier), touchant ainsi son activité et sa réputation.

Dans un établissement HCR, plusieurs collaborateurs peuvent avoir accès à plusieurs types de comptes (mails, backoffice de plateformes en ligne…). Quelques réflexes doivent être acquis par TOUS les collaborateurs, même ceux qui n'ont *a priori*, pas d'usages du numérique dans leurs taches.

La gestion des objets connectés

1. **Bien choisir ses mots de passe**

Un mot de passe doit comporter au moins 8 caractères avec des majuscules, des minuscules, des chiffres et si possible un caractère non-alphanumérique. Autant que possible il faut un mot de passe par utilisateur (et non pas uniquement par type de poste), et le changer régulièrement (2 fois par an) et au départ de la personne. Il faut également un mot de passe par type de connexion (pas le même pour le logiciel X et le réseau social !) Parmi les mots de passe les plus importants, **celui de la boite mail est le plus sensible**.

2. **Verrouiller les objets connectés**

Ordinateurs fixes ou portables, tablettes ou smartphones doivent être verrouillés manuellement dès que la personne qui l'utilise s'en éloigne. Pour s'assurer que ce verrouillage est effectué automatiquement, ces outils peuvent être paramétrés :

- 10 minutes sans activité pour un ordinateur fixe ;
- 5 minutes sans activité pour un ordinateur fixe ;
- 5 minutes sans activité pour un ordinateur portable ou une tablette ;
- 3 minutes sans activité pour un smartphone.

3. **Bien entretenir son système informatique**

Mettre régulièrement à jour les logiciels car des corrections sont apportées régulièrement aux failles de sécurité.

4. **Régulièrement effectuer des sauvegardes des données**

ET s'assurer qu'elles fonctionnent en les restaurants de temps en temps. Enfin toute nouvelle connexion, par exemple avec une clef USB, doit être analysée avec un anti-virus.

5. **Sécuriser ses objets connectés**

Un smartphone, une tablette, un ordinateur portable doivent être autant protégés qu'un ordinateur fixe. A minima **paramétrer un verrouillage automatique avec demande de mot de passe.** De même **un antivirus et un pare-feu** sont des éléments essentiels pour ces mini-ordinateurs qui comportent directement ou indirectement de nombreuses données confidentielles.

6. **Etre vigilent lors de l'utilisation de la messagerie**

Vérifier les expéditeurs, ne pas ouvrir les pièces jointes ou cliquer sur les liens automatiquement sans s'assurer du contenu. En cas de doute sur un mail reçu demandant des informations, chercher à joindre l'expéditeur pour s'assurer de la véracité du mail.

7. **Informer et former son personnel aux bons usages**

Il est important de veiller à ce que des conversations confidentielles ne soient pas entendues dans des espaces communs (train, hall d'hôtels, restaurant…)

8. **Séparer les usages personnels et professionnels**

Ne pas avoir un seul téléphone, une messagerie personnelle avec toutes les redirections des autres adresses mails professionnelles (ou inversement), ne pas connecter automatiquement son compte personnel sur un outil (téléphone, ordinateur) professionnel…

La gestion des espaces de connexion générique

1. **Limiter au maximum les espaces de connexion (mails…) génériques**

Il est préférable de créer un espace de connexion par collaborateur. Néanmoins dans un établissement CHR, des adresses génériques (adresse de réservation, relation client, backoffice de plateformes numériques…) sont souvent nécessaires. La sécurité et l'implication de chaque collaborateur sont donc deux éléments à renforcer dès le départ.

2. **Paramétrer les adresses mail sur un logiciel de messagerie (mailer)**

Et éviter les adresses mail sur une plateforme numérique comme Gmail, Yahoo, Orange… qui sont des adresses mails pour lesquelles la connexion peut facilement se faire sans logiciel de messagerie. Elles sont donc plus facilement utilisables en dehors de l'établissement. Il est donc préférable de créer des adresses mail via l'hébergeur du site web de l'établissement et de les paramétrer dans un logiciel de messagerie.

3. **Exiger le mot de passe à chaque utilisation du mailer**

Les mails ne doivent pas être accessibles à une personne ne connaissant pas le mot de passe.

Sensibiliser chaque collaborateur à la bonne gestion des données personnelles

La multiplication et la diversification des cybermenaces en font un phénomène complexe à appréhender pour le grand public.

Ainsi, Cybermalveillance.gouv.fr poursuit les travaux initiés en 2017 en créant avec ses membres un kit de sensibilisation qui adressera le particulier à travers le canal professionnel.

Réalisé sous licence ouverte (ETALAB 2.0), ce kit est mis gratuitement à disposition des entreprises, collectivités et associations. Il contiendra des outils pédagogiques adaptés et modulaires (vidéos, infographies, fiches réflexes, ...) à destination de leurs collaborateurs afin de :

- **Sensibiliser aux risques numériques**
- **Dispenser les bonnes pratiques**
- **Traiter des usages professionnels et personnels**

Les organisations qui participeront à cette opération contribueront à améliorer l'hygiène informatique de leurs collaborateurs tant dans leurs usages personnels que par voie de conséquence dans leurs usages professionnels.

Téléchargez ici le kit de sensibilisation : https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/

Retrouvez tous les conseils en cybersécurité pour les établissements HCR sur la rubrique dédiée du site du GHR : https://www.GHR-hcr.fr/europe-numerique/informatique/cybersecurite/

Modèles de documents GHR de communication

Envers les employés

A noter que seule l'obligation formelle d'informer ses collaborateurs est nouvelle. Toutes les obligations concernant la protection des données personnelles des salariés, hormis les déclarations préalables à la CNIL (vidéosurveillance, fichier de candidats… qui deviennent des informations à notifier aux individus), restent valables.

En cas de vidéosurveillance, reportez-vous à la partie concernée pour les clients ! *N'hésitez pas à demander au GHR la Fiche pratique sur la vidéosurveillance !*

De même dans le cas où l'établissement aurait en place un système de pointeuse (horaires de travail des salariés), celui-ci doit faire l'objet d'une fiche de traitement des données dans le Registre de protection des données.

Contrat de travail : avenant ou annexe

Dans le cadre de la gestion du personnel et de la paie, nous sommes amenés à collecter vos données personnelles (ex : nom, prénom, adresses, numéro de téléphone…). Elles font l'objet d'un traitement dont le responsable est (ajouter le nom et les coordonnées de l'entreprise).

Mme ou M. (ajouter le nom et les coordonnées) est la personne référente sur le sujet.

Ces données personnelles ne seront traitées ou utilisées que dans la mesure où cela est nécessaire pour :

1) exécuter votre contrat de travail :
ex : utilisation de vos coordonnées bancaires pour vous verser votre salaire,
ex : utilisation de votre adresse postale pour vous envoyer des courriers,
ex : utilisation de votre numéro de téléphone et votre adresse mail professionnels pour pouvoir vous joindre pendant le temps de travail,
ex : utilisation de vos noms, prénom et coordonnées professionnelles pour mettre à votre disposition des équipements informatiques et/ou de télécommunications,
autres …

ET

2) répondre à une obligation légale et/ou réglementaire :
ex : utilisation de vos noms, prénoms, date et lieu de naissance, numéro de sécurité sociale pour la DPAE (déclaration préalable à l'embauche), et la DSN (déclaration sociale nominative) auprès de l'URSSAF,
ex : utilisation de votre photo pour établir votre carte professionnelle,
ex : utilisation de votre situation matrimoniale et du nombre d'enfants pour vous inscrire aux régimes prévoyance et frais de santé,
autres …

Vos informations personnelles seront conservées aussi longtemps que nécessaire à l'exécution de votre contrat [OU indiquer une durée de conservation des données], à

l'accomplissement par l'entreprise de ses obligations légales et réglementaires et à l'exercice des prérogatives lui étant reconnues par la loi et la jurisprudence.

Pendant toute la durée de conservation de vos données personnelles, nous mettons en place tous les moyens aptes à assurer leur confidentialité et leur sécurité, de manière à empêcher leur endommagement, effacement ou accès par des tiers non autorisés.

L'accès aux données personnelles est strictement limité aux salariés de l'entreprise, habilités à les traiter en raison de leurs fonctions. Les informations recueillies pourront éventuellement être communiquées à des tiers liés à l'entreprise par contrat pour l'exécution de tâches sous-traitées nécessaires à la gestion de votre contrat (ex la société X à qui nous avons sous-traité la paie).

Il est précisé que, dans le cadre de l'exécution de leurs prestations, les tiers n'ont qu'un accès limité aux données et ont l'obligation de les utiliser en conformité avec les dispositions de la législation applicable en matière de protection des données personnelles.

Les destinataires des données sont intégralement situés au sein de l'Union européenne.

Conformément aux dispositions légales et règlementaires applicables, vous bénéficiez d'un droit d'accès, de rectification, de portabilité et d'effacement de vos données ou encore de limitation du traitement. Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant. Vous pouvez, sous réserve de la production d'un justificatif d'identité valide, exercer vos droits, et vous opposer au traitement des données vous concernant et disposez du droit de retirer votre consentement à tout moment en en contactant (préciser les modalités : par mail par courrier… et insérer les noms et coordonnées du service ou de la personne compétente).

En cas de difficulté en lien avec la gestion de vos données personnelles, vous pouvez contacter la Commission nationale de l'informatique et des libertés (plus d'informations sur www.cnil.fr).

Le XXXXXXXX

A XXXXXX

Signature du chef d'entreprise *Signature du salarié*

Note interne

La note interne sera un document identique à cet avenant/annexe au contrat de travail (sans la signature du salarié)

Règlement intérieur

Le texte de l'avenant/annexe au contrat de travail peut être ajouter au sein ou en annexe du Règlement intérieur en ajoutant une phrase sur les sanctions encourues en cas de l'absence de respect de l'engagement de confidentialité pour les personnes ayant vocation à manipuler des données à caractère personnel au sein de l'établissement.

En cas de badges d'accès horodatés

Si l'établissement remet des badges d'accès aux employés, une sous-rubrique « Accès par badge » doit être ajoutée à la rubrique « Protection des données personnelles » du Règlement intérieur.

> *L'établissement [Nom de l'établissement] a mis en place un système non biométrique d'accès par badge afin de contrôler l'accès à ses locaux. La base légale du traitement est l'intérêt légitime (cf. article 6.1.f) du Règlement européen sur la protection des données).*
>
> *Données enregistrées sur les employés de la société ABCD :*
> *Identité : nom, prénom, numéro de matricule interne, service, photographie.*
> *Badge : numéro du badge, date de validité.*
> *Date et heures d'entrée et de sortie.*
>
> *Date et heures d'entrée dans une pièce spécifique (chambre, réserve, …) [à préciser selon l'établissement] en fonction des droits d'accès définis par le poste occupé.*
>
> *Destinataires des données :*
> *Les personnes habilitées du service du personnel.*
> *Les personnes habilitées du service gérant la sécurité des locaux.*
> *Durée de conservation des données : 3 mois.*
>
> *Droits des personnes :*
>
> *Vous pouvez accéder aux données vous concernant ou demander leur effacement. Vous disposez également d'un droit d'opposition, d'un droit de rectification et d'un droit à la limitation du traitement de vos données (cf. cnil.fr pour plus d'informations sur vos droits).*
>
> *Pour exercer ces droits ou pour toute question sur le traitement de vos données dans ce dispositif, vous pouvez contacter notre délégué à la protection des données (DPO).*
>
> *Contacter la personne responsable par voie électronique : [les noms et coordonnées du service ou de la personne compétente].*
>
> *par courrier postal : [coordonnées de l'établissement avec les noms du service ou de la personne compétente]*
>
> *Si vous estimez, après nous avoir contactés, que vos droits Informatique et Libertés ne sont pas respectés ou que le dispositif de contrôle d'accès n'est pas conforme aux règles de protection des données, vous pouvez adresser une réclamation en ligne à la CNIL ou par voie postale.*

Voir également les recommandations pour les clients.

En cas de pointeuse

Si l'établissement met en place une pointeuse pour ses salariés, cette activité doit faire l'objet d'une fiche de traitement des données dans le Registre de protection. En revanche il n'est pas nécessaire de faire une déclaration à la CNIL.

Concernant l'information à diffuser aux salariés, il est nécessaire de transmettre une note explicative comprenant les éléments ci-dessous à **chaque** salarié :

- Les motifs de la collecte (= l'intérêt légitime de l'employeur),
- Les personnes qui auront accès à ces données (surtout si elles sont stockées sur un cloud ou via les serveurs du prestataire en vérifiant alors que les serveurs sont bien sur le territoire de l'UE),
- La durée de conservation (la recommandation CNIL est de 3 mois pour les accès, de 5 ans pour le suivi du temps de travail notamment les données relatives aux motifs des absences),
- Les moyens de sécurisation de ces données (à vérifier avec le prestataire de la pointeuse),
- Rappel du droit d'accès, modification et suppression de ces données collectées (uniquement sur motif légitime) avec les coordonnées de la personne en interne à contacter,
- La possibilité de faire une réclamation à la CNIL.

En cas de vidéosurveillance

A noter que la vidéosurveillance doit faire l'objet d'une fiche de traitement des données dans le Registre de protection. En revanche il n'est pas nécessaire de faire une déclaration à la CNIL.

Le RGPD réclame que les solutions choisies face aux enjeux soient les moins intrusives possible. La vidéo-surveillance doit donc être exclusivement mise en place pour la protection des biens et des personnes. Les caméras doivent donc viser les accès ; éventuellement vers les biens le plus précieux, mais jamais le personnel. Il est interdit notamment de positionner une caméra au-dessus d'une pointeuse ou dans la salle de pause.

N'hésitez pas à demander au GHR la Fiche pratique sur la vidéosurveillance notamment pour connaître les modalités de déclaration à la Préfecture !

Concernant l'information à diffuser aux salariés, il est nécessaire de transmettre une note explicative comprenant les éléments ci-dessous à **chaque** salarié :

- Les motifs de la collecte (= l'intérêt légitime de l'employeur),
- Les personnes qui auront accès à ces données (surtout si elles sont stockées sur un cloud ou via les serveurs du prestataire en vérifiant alors que les serveurs sont bien sur le territoire de l'UE),
- La durée de conservation (la recommandation CNIL est de 1 mois),
- Les moyens de sécurisation de ces données,
- Rappel du droit d'accès, modification et suppression de ces données collectées (uniquement sur motif légitime) avec les coordonnées de la personne en interne à contacter,
- La possibilité de faire une réclamation à la CNIL.

Voir également les recommandations pour les clients.

Engagement de confidentialité

Avec ce modèle, les personnes ayant vocation à manipuler des données à caractère personnel au sein de l'établissement, prennent l'engagement de respecter la confidentialité des données collectées et traitées. Cet engagement doit donc être signé par les employés ayant accès aux données personnelles des autres salariés, des

clients, prospects et fournisseurs. Une phrase indiquant les sanctions en cas d'irrespect de cet engagement peut être insérée dans le Règlement intérieur.

Je soussigné/e Monsieur/Madame,

Exerçant les fonctions de XXXXXXXXXX au sein de la société (ci-après dénommée « la Société »), étant à ce titre amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations aux- quelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- *ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;*
- *ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;*
- *ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;*
- *prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;*
- *prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;*
- *m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces don- nées ;*
- *en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.*

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.
J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Fait à xxx, le xxx, en xxx exemplaires. *Nom* *Signature*

Information du candidat à l'embauche

En cas de collecte des candidatures par voie numérique, ce document doit être utilisé comme modèle d'information avant l'envoi de la candidature en étant validé deux fois en guise de signature.

Merci de bien vouloir lire et compléter soigneusement le présent formulaire.

Veuillez noter que les réponses aux cases munies d'un astérisque sont obligatoires et nécessaires au bon traitement de votre candidature. Les informations personnelles portées sur ce formulaire font l'objet d'un traitement informatisé (ou non-informatisé) dont le responsable est (ajouter le nom et les coordonnées de l'entreprise).

[Si l'entreprise fait passer des tests particuliers dans le cadre du processus d'embauche] Conformément aux dispositions légales et réglementaires en vigueur, nous vous informons que la politique de recrutement de notre entreprise comprend (préciser les tests mis en œuvre : tests graphologiques et/ou épreuves d'essai, etc.). Les résultats de ces tests vous seront restitués sur demande et uniquement conservés dans votre dossier salarié en cas d'embauche.

Nous ne traiterons ou n'utiliserons vos données que dans la mesure où cela est nécessaire pour vous contacter et assurer le bon traitement de votre candidature. Les informations personnelles collectées seront conservées au maximum deux ans à compter du dernier contact de l'entreprise avec vous.

L'accès aux données personnelles est strictement limité aux salariés de l'entreprise, habilités à les traiter en raison de leurs fonctions. Les informations recueillies pourront éventuellement être communiquées à des tiers liés à l'entreprise par contrat pour l'exécution de tâches sous-traitées nécessaires au traitement de votre candidature, sans que votre autorisation soit nécessaire. Il est précisé que, dans le cadre de l'exécution de leurs prestations, les tiers n'ont qu'un accès limité aux données et ont l'obligation de les utiliser en conformité avec les dispositions de la législation applicable en matière de protection des données personnelles.

Les destinataires des données sont intégralement situés au sein de l'Union européenne

Conformément aux dispositions légales et règlementaires applicables, vous bénéficiez d'un droit d'accès, de rectification, de portabilité et d'effacement de vos données ou encore de limitation du traitement. Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant. Vous pouvez, sous réserve de la production d'un justificatif d'identité valide, exercer vos droits en contactant (préciser les modalités : par mail par courrier… et insérer les noms et coordonnées du service ou de la personne compétente).

En cas de difficulté en lien avec la gestion de vos données personnelles, vous pouvez adresser une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés ou de toute autre autorité compétente.

Le XXXXX , A XXXXXXXXXXX *Nom et Signature du candidat*

Envers les clients

Mail aux anciens clients

Les bases de données des établissements HCR contiennent un certain nombre de données d'anciens clients. Certaines données sont à conserver (voir les durées légales de conservation), mais d'autres peuvent être supprimées. Tous les clients doivent pouvoir modifier ou supprimer leurs données personnelles dans la limite des durées légales. Le mail ci-dessous permet à l'établissement de respecter son engagement de libre accès à leurs données personnelles.

En français :

> *Chère cliente, cher client,*
>
> *Le 25 mai 2018 le Règlement général sur la protection des données personnelles est entré en vigueur en France.*
>
> *Une fiche client comprenant certaines de vos données personnelles a été créée pour réaliser notre prestation de [restauration/hébergement]. Par ce mail nous souhaitons vous informer que notre établissement met tout en œuvre pour respecter la réglementation de protection des données personnelles, notamment par un niveau de sécurité élevé de nos données informatiques et en ayant reçu toutes les garanties de la part de nos sous-traitants du bon respect de ces obligations.*
>
> *Sachez que vous pouvez, en contactant [email du DPO et/ou de la personne responsable des données clients et/ou un email générique dédié à la protection des données] :*
> *- Nous demander la modification de vos données personnelles.*
> *- Nous demander la suppression de votre mail de nos newsletters. Attention, en vous désinscrivant, vous risquez de ne plus avoir connaissance d'éventuelles promotions qui pourraient vous intéresser.*
> *- Nous demander la suppression de l'intégralité de votre fiche client, dans la limite des durées légales de conservation des données.*
>
> *Par cet email nous nous tenons à votre entière disposition pour vous détailler les éventuels traitements auxquels vos données personnelles sont soumises.*
>
> *Sachez que sans aucun retour de votre part, nous conserverons vos données personnelles à des fins de prospection commerciale au maximum pendant 3 ans à compter de la dernière relation eue avec nos services.*
>
> *Nos conditions générales de vente mises à jour sont disponibles en cliquant ici.*
>
> *En vous remerciant pour votre confiance,*
>
> *XXX,*
>
> *Directeur de l'établissement YYY*

En anglais :

Dear guest,

On May 25th 2018, the General Data Protection Regulation (GDPR) came into effect in France. A guest profile containing some of your personal data has been created for our hosting purposes.

This email is to inform you that our hotels are making sure that they abide by the GDPR, notably through implementing a high level of data security, for which our sub-contractors have given us full guarantee that they will respect their obligations. You can contact XXX,

Should you wish to:

- *Ask us to modify your personal data*
- *Unsubscribe from our newsletters (if you unsubscribe, you may not be aware of promotions that might be of interest to you)*
- *Ask us to delete your guest profile data, within the legal limits of data storage*

We are at your entire disposal to inform you of the way your personal data may be used.

Without any intervention on your part, we will keep your personal data for marketing purposes for a maximum of 3 years after our last commercial relationship with you. Our updated general sales conditions are available by clicking here.

We thank you for your business.

Clause dans les conditions générales de vente

Si votre établissement possédait déjà une clause informant de la protection des données, il n'est pas nécessaire de suivre le modèle proposé ci-dessous. Il vous faut cependant vérifier que la clause contient :

- Le droit à l'accès, modification, suppression et opposition à un traitement spécifique aux données personnelles collectées pour permettre la prestation hôtelière/de restauration.
- L'information sur comment ou auprès de qui faire usage de ces droits d'accès, modification, suppression et opposition.
- L'information sur l'utilisation qui est faite de ces données personnelles.
- L'information sur les structures qui utilisent ces données personnelles dans le cadre de la prestation hôtelière/de restauration.

Avec le RGPD il est préférable, si vous êtes concernés, d'ajouter les liens vers les documents fournis par tout ou partie des sous-traitants (voir ici le modèle de demande) utilisant les données personnelles des clients avec une phrase du type :

> *« Certaines données personnelles peuvent être collectées pour des services fournis par des prestataires de l'hôtel. Retrouvez ici leurs documents relatifs à la protection des données à caractère personnel des utilisateurs : [Liste des prestataires concernés avec lien vers les informations] »*

Si votre établissement ne possédait pas de clause sur la protection des données personnelles dans vos Conditions générales de vente, voici un modèle pour un établissement HCR :

> ***« Données personnelles » :***
> *Toute prestation fera l'objet d'un enregistrement accessible par le Client sur simple demande à l'adresse suivante [indiquer l'adresse mail du responsable de traitement signalé dans le Registre de protection des données ou à défaut une adresse mail dédiée]*
> *Conformément à la Loi 78-17 « Informatique et Libertés » du 6 janvier 1978 modifiée, les clients disposent d'un droit d'accès, de rectification et d'opposition aux données personnelles traitées les concernant.*
> *Le Client peut également refuser le traitement, solliciter une limitation de celui-ci ou demander la suppression (dans les limites des durées légales de conservation) des données à caractère personnel.*
> *Ce droit peut être exercé sur simple demande écrite à [adresse mail] qui répondra aux demandes formulées.*
> *La finalité du traitement des données personnelles collectées correspond aux obligations relatives aux prestations réalisées (gestion clients, prospection commerciale… [à compléter si nécessaire])*
> *Les données personnelles seront conservées à des fins de prospection commerciale au maximum pendant 3 ans à compter de la dernière relation eue avec nos services.*
>
> *[A ajouter si vous êtes concernés] :*
> *Certaines données personnelles peuvent être collectées pour des services fournis par des prestataires de l'hôtel. Retrouvez ici leurs documents relatifs à la protection des données à caractère personnel des utilisateurs : [Liste des prestataires concernés avec lien vers les informations]*

Pour mémoire tous les sites internet doivent contenir une page de mentions légales, accessible à partir de toutes les pages du site. Pour connaitre le contenu à y indiquer, cliquer ici pour consulter le site du Service public.

En cas d'absence de Conditions générales de vente, ces mentions doivent apparaître sur tout support de communication avec le consommateur.

Il est également possible de rappeler ces mentions dans les mails ou factures, en indiquant uniquement le paragraphe :

> *Conformément à la Loi 78-17 « Informatique et Libertés » du 6 janvier 1978 modifiée, les clients disposent d'un droit d'accès, de rectification et d'opposition aux données personnelles traitées les concernant. Pour plus d'informations consulter l'article XXX des Conditions générales de vente.*

Demande de consentement pour toute fourniture de données

La clause contenue dans les Conditions générales de vente est éventuellement à décliner sur tous les autres supports commerciaux grâce auxquels l'établissement collecte des données personnelles, en direct ou via un prestataire gérant également ces données personnelles (CRM, Cabinet comptable…). Voici quelques exemples précis, qui sont néanmoins duplicable pour tous les services.

Saisie d'email par un sous-traitant

Lors d'une demande de saisie d'email par un sous-traitant CRM, un fournisseur de WiFi… :

> « Ce service vous est fourni par notre partenaire XXX. [Consultez ici la Charte relative à la protection des données à caractère personnel des utilisateurs de XXX.] »

A noter : Si vous collectez l'adresse mail pour un autre usage que le WiFi (par exemple pour ajouter l'adresse mail à la fiche client), l'information doit être donnée à la personne *(« Votre adresse mail sera également utilisée par l'hôtel YYY pour toute information relative à votre séjour »*). Cette adresse mail ne pourra pas être utilisée pour envoyer des informations marketing sauf à y ajouter la mention disponible à l'Exemple 3.

Envoi de l'email pré/post-séjour par un prestataire

Lors d'une demande d'adresse mail pour envoi d'informations pré- et/ou post-séjour si c'est effectué par un prestataire notamment :

> *« Dans le cadre de notre prestation hôtelière/de restauration, votre adresse mail sera utilisée par l'établissement YYY pour vous envoyer des informations concernant votre réservation et votre séjour. »*
>
> *« Ce service vous est fourni par notre partenaire XXX. [Consultez ici la Charte relative à la protection des données à caractère personnel des utilisateurs de XXX.] »*

Inscription ou utilisation de l'email pour une newsletter

Il est nécessaire de demander le consentement pour l'utilisation de l'adresse mail pour envoi d'une newsletter ou d'offres promotionnelles (à mettre dès le formulaire de collecte de l'email) :

> *« Vous acceptez que votre adresse mail soit utilisée par l'établissement YYY pour vous envoyer des offres promotionnelles [et/ou] une newsletter [hebdomadaire/mensuelle/trimestrielle…]. »*

A noter : les cases à cocher pour accepter l'utilisation des adresses mails, des numéros de téléphone ou autre donnée personnelle dans le cadre d'envoi de newsletter ou emailings commerciaux doivent être par défaut décochées. En cas de gestion par un prestataire (collecte et/ou envoi) qui conserve également ces données, il faut coupler cette phrase avec l'exemple 1.

En cas de vidéosurveillance

A noter que la vidéosurveillance doit faire l'objet d'une fiche de traitement des données dans le Registre de protection des données. En revanche il n'est pas nécessaire de faire une déclaration à la CNIL.

Le RGPD réclame que les solutions choisies face aux enjeux soient les moins intrusives possible. La vidéo-surveillance doit donc être exclusivement mise en place pour la protection des biens et des personnes. Les caméras doivent donc viser les accès ; éventuellement vers les biens le plus précieux, mais jamais le personnel.

N'hésitez pas à demander au GHR la Fiche pratique sur la vidéosurveillance notamment pour connaître les modalités de déclaration à la Préfecture !

Concernant la vidéosurveillance des espaces publics, un affichage doit être mis à disposition, en suivant ce modèle :

> *« Etablissement placé sous vidéosurveillance par Nom de l'établissement pour la sécurité des personnes et des biens.*
>
> *Les images sont conservées pendant un mois et peuvent être visionnées, en cas d'incident, par le personnel habilité de Nom de l'établissement et par les forces de l'ordre.*
>
> *Pour exercer vos droits Informatique et Libertés, notamment votre droit d'accès aux images qui vous concernent, ou pour toute information sur ce dispositif, vous pouvez contacter notre responsable de traitement des données, en écrivant à adresse mail ou à l'adresse postale suivante : XXXX. »*

Voir également les recommandations pour les salariés.

En cas de badges d'accès horodatés

Si l'établissement remet des badges d'accès par exemple aux chambres et/ou aux espaces communs (piscine, espace bien-être…) une sous-rubrique « Accès par badge » doit être ajoutée à la rubrique « Protection des données personnelles » des conditions générales de vente.

> *Afin de contrôler l'accès à ses locaux, l'établissement [nom de l'établissement] sécurise les accès des chambres et de certains espaces communs [à préciser si nécessaire] à ses résidants à l'aide d'un badge remis lors de l'arrivée dans l'établissement.*
>
> *Les données enregistrées dans ce dispositif d'accès aux locaux sont conservées pendant trois mois et sont accessibles au personnel en charge de la sécurité et la direction.*
>
> Pour exercer vos droits Informatique et Libertés et pour toute information sur ce dispositif, contactez notre responsable à la protection des données (DPO) [préciser le nom du service ou de la personne et son titre] *en écrivant à adresse mail ou à l'adresse postale suivante : XXXX. »*

Voir également les recommandations pour les salariés.

Fiches clients

Zones de commentaires libres

Certains PMS mettent à disposition une zone de commentaires libres afin de rédiger des notes subjectives sur le client. Il est préférable de les limiter et de favoriser les listes de mots clefs. Il est également nécessaire d'en informer le client.

Conservation des choix de commande

Pour toute conservation de données facultatives, il est nécessaire de donner le choix et d'obtenir le consentement clair et explicite :

> *« Acceptez-vous que vos préférences et/ou votre commande, soient enregistrées et conservées pour une prochaine venue dans notre établissement ? »*

A noter que si ces données sont conservées uniquement dans un objectif de statistiques il est préférable de ne pas les liées aux profils des clients.

Si les informations concernent un handicap ou une allergie, il s'agit alors de données sensibles. Il est alors obligatoire, de demander le consentement, idéalement par écrit, au client s'il souhaite que ces données soient conservées afin de lui apporter un service adéquat lors d'une prochaine visite. La conservation de ces données devra également faire l'objet d'une sécurité adaptée.

Autres

Mail aux fournisseurs

Les fournisseurs des établissements sont ici toutes les structures qui permettent la gestion de l'établissement sans traiter de données personnelles d'employés ou de clients. Il peut s'agir des sociétés fournissant les denrées alimentaires, les livreurs, les sociétés s'occupant du nettoyage (lingerie, ménage…). Au sein de l'activité qu'ils mènent sous contrat avec votre établissement, il est possible que des données personnelles (nom, prénom, téléphone, mail…) vous soient communiquées. Ils bénéficient à ce titre des mêmes droits que vos employés et clients/prospects et doivent donc être informés du traitement de leurs données personnelles.

Madame, Monsieur,

Le 25 mai 2018 le Règlement général sur la protection des données personnelles entre en vigueur en France.

Une fiche fournisseur comprenant certaines de vos données personnelles a été créée dans le cadre de notre contrat [nom et/ou numéro du contrat]. Par ce mail nous souhaitons vous informer que notre établissement met tout en œuvre pour respecter la réglementation de protection des données personnelles, notamment par un niveau de sécurité élevé de nos données informatiques et en ayant reçu toutes les garanties de la part de nos sous-traitants du bon respect de ces obligations.

Sachez que vous pouvez, en contactant [email du DPO et/ou de la personne responsable des données clients et/ou un email générique dédié à la protection des données] :

- Nous demander la modification de vos données personnelles.

- Nous demander la suppression de l'intégralité de votre fiche fournisseur, dans la limite des durées légales de conservation des données.

Par cet email nous nous tenons à votre entière disposition pour vous détailler les éventuels traitements auxquels vos données personnelles sont soumises.

Sachez que nous attendons de votre part ce même degré de respect de la réglementation des données personnelles nous concernant.

En vous remerciant pour votre confiance,

XXX,

Directeur de l'établissement YYY

Mail aux sous-traitants

Vos sous-traitants sont les structures qui gèrent certains services que vous proposez aux clients, qu'ils soient numériques ou non. Cela peut être

- Un distributeur (OTA, plateforme de réservation, agences de voyage…),
- Un prestataire de relation clientèle (CRM, gestionnaire d'e-reputation, agence marketing…),
- Un prestataire de logiciel qui héberge vos données (PMS…),
- Un prestataire de comptabilité-gestion (cabinet comptable gérant les bulletins de paie…),
- Un prestataire de télésurveillance

Ces sous-traitants traitent tout ou partie des données personnelles de l'établissement (employés et/ou clients) et dans ce cadre, ils doivent s'être mis en conformité avec le RGPD en vous précisant :

- Les clauses contractuelles modifiées entre le sous-traitant et votre établissement
- L'éventuel document d'information à communiquer aux employés/clients qui utilisent leurs services à travers votre établissement,
- Le nom et les coordonnées du contact responsable du traitement des données dans leur structure,
- La localisation de leurs serveurs informatiques.

Ces informations vous seront nécessaires pour le Registre de protection des données et pour en informer vos employés et/ou vos clients.

> *Madame, Monsieur,*
>
> *Le 25 mai 2018 le Règlement général sur la protection des données personnelles entre en vigueur en France.*
>
> *Sauf erreur de ma part, nous n'avons pas eu connaissance des nouvelles clauses contractuelles nous permettant de nous assurer, et de garantir à nos clients, que vous respectez bien l'ensemble de vos obligations s'agissant de ce Règlement générale sur la protection des données personnelles.*
>
> *Merci de nous faire parvenir au plus vite l'avenant à notre contrat comprenant les différentes clauses obligatoires citées par la CNIL (https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses).*
>
> *Afin d'être totalement conforme au Règlement européen, je vous prie de nous faire parvenir également au plus vite le cas échéant :*
> *- l'éventuel document d'information à communiquer aux employés/clients qui utilisent leurs services à travers votre établissement,*
> *- le nom et les coordonnées du contact responsable du traitement des données dans leur structure,*
> *- la localisation de leurs serveurs informatiques*
>
> *En vous remerciant pour votre diligence,*
>
> *XXX,*
>
> *Directeur de l'établissement YYY*

En cas de vol de données personnelles

Les actions à mettre en place

Si malheureusement votre établissement a été victime d'une attaque voici les étapes à suivre :

1. **Sécuriser immédiatement votre système informatique via votre prestataire habituel.** Votre prestataire doit vérifier l'ampleur de l'attaque, le périmètre des données compromises, et vous proposer des mesures de sécurité pour remédier au problème rencontré. Il doit également conserver les preuves de l'attaque afin de vous permettre de porter plainte.

2. **Porter plainte au commissariat le plus proche** et récupérer une attestation de plainte. En cas de refus catégorique du commissariat (certains étant peu à même de comprendre les problématiques numériques et les lourdes conséquences dans la société…) le GHR vous invite à écrire une Lettre plainte au Procureur de la République.

3. **Faire une première déclaration CNIL dans les 72h** si des données personnelles sont susceptibles d'avoir été volées. Formulaire en ligne disponible ici. Il faudra indiquer tout ce qui a été déjà été fait et si possible tout ce qui est en cours de réalisation. Cliquer ici pour plus d'informations sur les démarches CNIL. Pour plus d'aide vous pouvez également contacter Info Escroqueries au 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 euros/minute depuis un téléphone mobile) - Du lundi au vendredi de 9h à 18h

4. **Prévenir les personnes (clients, collaborateurs…) concernées (ou potentiellement concernées) par le vol de données** par un mail ou courrier (en cas d'absence d'adresse mail) en mentionnant tout ce qui a été fait immédiatement, voire en les invitant à eux-mêmes faire le nécessaire. Le GHR vous propose un modèle pour vous accompagner en pèce jointe à cet article (également disponible dans le Guide RGPD mis à jour). Non seulement cette information est une obligation légale, mais cela pourrait être déterminant pour la CNIL.

5. **Faire vérifier le système informatique de l'établissement par un audit extérieur**. En effet, sans préjugé des compétences du prestataire habituel, l'établissement doit pouvoir prouver que tout a été mis en œuvre pour éviter que l'incident ne se reproduise. L'audit est important pour s'assurer qu'aucun malware, logiciel malveillant n'a été installé sur vos postes lors du piratage rendant les changements de mots de passe inutiles… puisque visible par le hacker… Cela vous donne par ailleurs un document attestant de votre prise en main du problème. Un prestataire peut être trouvé sur cybermalveillance.gouv.fr OU pour les grands comptes (dans la rubrique RGS) : https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf

6. **Consulter la plateforme cybermalveillance.gouv.fr** pour obtenir un support complémentaire.

Courriel de notification aux clients de violation de données personnelles

Madame, Monsieur,

Notre établissement [*nom de l'établissement*] a été victime d'un piratage informatique en date du [*date*], certaines de vos données personnelles que vous nous aviez confiées en direct ou que nous avons collectées via notre distributeur [*liste des sous-traitants ciblées*] ont été [*potentiellement*] dérobées.

Il s'agit :

- de votre nom et de votre prénom ;
- de votre numéro de téléphone mobile ;
- de votre adresse courriel ;
- [*ajouter toutes les données concernées*]
- de votre numéro de carte bancaire.

Ces informations ont été communiquées par vous ou un proche lors d'une réservation dans notre établissement entre le [*date*] et le [*date*].

Sachez que le [*nom de l'établissement*] a tout mis en œuvre pour circonscrire cet incident et éviter que cela puisse se reproduire tant sur un plan technique que juridique.

Nous avons effectué un signalement à la CNIL comme la loi nous le demande. Une vérification informatique complète a également été réalisée. Pour sécuriser les données personnelles et éviter toute nouvelle fuite, notre établissement a notamment [Préciser tous les actions complémentaires mises en œuvre]

Néanmoins, il ne peut être exclu que ces données puissent être utilisées par des tiers à des fins publicitaires (par courriels ou sms), d'hameçonnage (« phishing ») ou de tentatives d'escroquerie.

Nous vous invitons à vous montrer vigilant si vous recevez des messages de source douteuse, qui vous inviteraient à préciser des informations personnelles ou des données d'identification, à ouvrir une pièce jointe ou encore à cliquer sur un lien vers un site internet.

Nous vous invitons également à vous rapprocher de votre banque pour faire le nécessaire et surveiller tout usage frauduleux de votre carte bancaire.

Si vous avez des questions concernant cet incident, vous pouvez nous contacter à [*adresse mail dédiée à la gestion des données personnelles*]

Le [*nom de l'établissement*] met au cœur de sa gestion la protection des données personnelles et la sécurité de ses installations informatiques. Nous vous présentons toutes nos excuses pour cet incident de sécurité et vous prions de croire que nous mettons tout en œuvre pour en limiter les effets et faire en sorte que cela ne puisse se reproduire.

Votre confiance est importante pour nous.

[*Signature*]

Directeur de [*nom de l'établissement*]

Vérifier sa conformité

D'après le texte du RGPD, les établissements du secteur de l'hôtellerie-restauration n'ont pas l'obligation de fournir une analyse d'impact, puisque la gestion des données personnelles ne constitue pas un risque élevé concernant les droits et les libertés des individus. Néanmoins, le tableau suivant donne la possibilité aux établissements d'évaluer leur conformité à l'ensemble des obligations.

Etapes	oui/non	Commentaires
D'identifier et de recenser les données à caractère personnel qui sont stockées et/ou traitées et dont il a connaissance		
De se poser la question de la pertinence de conserver et/ou traiter ces données et de la pertinence de la finalité des traitements		
De se poser la question de la sécurité attachée à l'intégrité, à la confidentialité et à l'accès des données		
De vérifier que ces données ne sont pas des données sensibles (race, religion, …) et que ces personnes concernées sont informées de la détention et/ou du traitement de ces données et qu'elles ont donné leur accord		
Analyser à l'aide de fiches les traitements et les données		
Effectuer une analyse de risque et, si le risque est élevé, une analyse d'impact sur la vie privée (voir outil CNIL)		
De signaler aux personnes concernées et, dans les 72h à la CNIL toute disparition ou violation concernant ces données		
Réviser les contrats de travail pour inclure de manière explicite le consentement sur l'utilisation des données personnelles à des fins assez larges comme la gestion de carrière, les évaluations annuelles, les photos sur des posters, les annuaires internes, etc.		
Réviser le règlement intérieur afin de généraliser l'utilisation des données personnelles des salariés et de prévenir l'utilisation de données personnelles sensibles		
Réviser les Conditions Générales de Vente pour prendre en compte la prévention des données à caractère personnel selon le règlement		
Informer les sous-traitants informatiques de leurs responsabilités en matière de traitement de données personnelles et mise en place d'avenants aux contrats		

Informer au fil de l'eau des tiers s'il y a échange de données personnelles, mention spécifique à insérer dans les modèles de contrat et mise en place éventuelle d'avenants aux contrats		
Analyser les échanges hors Europe de données personnelles en fonction des pays et des finalités de traitement		
Définir les modalités d'accès aux informations par les personnes concernées aux fins d'information, de rectification, d'effacement, de limitation de traitement ou de portabilité.		
Organiser la Gouvernance, responsable et/ou DPO à désigner, code de conduite à rédiger.		
Documentation à conserver de toutes ces étapes, dossier numérique RGPD à organiser, Registre et fiches registre à tenir à jour.		
Mettre à niveau si besoin la sécurité informatique en relation avec les données		
Contrôler l'accès aux données de façon adaptée, accès en local ou à distance		
Imposer l'authentification et des mots de passe sécurisés		
Stocker et communiquer les informations sensibles de manière sécurisée (chiffrement)		
Appliquer une sécurité rigoureuse sur les nouveaux traitements		
S'assurer que les prestataires de services mettent en place des mesures de sécurité informatique		
Avoir des procédures de maintien de la sécurité et de correction des vulnérabilités.		

Blockproof : partenaire du GHR sur le RGPD

En mars 2021 le GHR est fier de vous annoncer la signature d'une convention avec **un nouveau partenaire qui permet aux établissements HCR d'accélérer leur conformité au RGPD : Blockproof**. Cette solution consiste à **concevoir simplement et rapidement son Registre de protection des données personnelles et à sauvegarder l'intégralité du dossier de conformité** de votre établissement. Le tout… avec des tarifs préférentiels exclusifs pour les adhérents du GHR.

La solution Blockproof

Le registre de protection des données personnelles

Blockproof est une solution numérique qui vous permet de **concevoir simplement et rapidement votre Registre de protection des données personnelles.** Le parcours de conception du registre est guidé, des suggestions automatiques vous sont proposées en fonction de votre métier avec la possibilité de les adapter à l'évolution de votre établissement.

Le remplissage est dès lors très simple. Il suffit :

1. de lister les activités (relatives aux données personnelles par ex : gestion de la paie, gestion de la distribution…)à partir des suggestions,
2. de choisir si votre établissement est concerné par telle ou telle donnée,
3. de renseigner les différents interlocuteurs de la gestion des données (qu'ils soient en interne ou en externe)
4. de préciser à partir des listes déroulantes, quelques informations sur chaque type de données collectées (finalités, origine, destinataires potentiels…) …

A partir des informations remplies par le responsable des données (ou une autre personne détenant les informations requises), **la solution propose un Registre de protection des données conforme aux normes de la CNIL** ainsi que d'autres mises en page plus ergonomiques pour le gérant pour comprendre et suivre l'ensemble des données personnelles collectées afin d'en faciliter leur gestion. Ces registres sont bien entendu téléchargeables et présentables comme preuve en cas de contrôle.

Le dossier de conformité au RGPD

La solution Blockproof propose également de **sauvegarder l'intégralité de votre dossier de conformité au RGPD**. Pour cela des modèles de documents d'information vous sont proposés afin de vous permettre de les « personnaliser » à l'image de votre établissement puis de stocker ces preuves d'information (jusqu'à 10 Go) ces preuves d'information de manière sécurisée.

Option Offre Site Web

Blockproof vous permet également (sur option) de mettre à jour votre site web pour le rendre conforme au RGPD. En effet pour la CNIL, c'est le site web qui est la vitrine de l'établissement pour savoir si le RGPD est respecté ou non. Blockproof vous accompagne pour mettre à jour vos Mentions légales (pour rappel cette rubrique est obligatoire et doit être accessible à partir de toutes les pages du site), les Cookies, et votre Politique de protection des données (souvent dans vos CGV qui doivent également se trouver sur votre site web).

Découvrez ici le fonctionnement de Blockproof.

4 rue de Gramont 75002 PARIS
T 01.42.96.60.75

Le partenariat entre le GHR et Blockproof

Une solution dédiée aux établissements HCR

L'équipe de Block-it a travaillé avec le GHR sur le développement de la solution Blockproof pour proposer une **ergonomie spécifique aux établissements du secteur HCR**. En 2019, deux hôteliers ont ainsi testé la solution en réel pour leurs établissements et donné les orientations sur les éléments indispensables à insérer dans un registre de protection des données des hôtels. En 2021 ce sont 3 restaurateurs qui testeront la solution afin d'en garantir son efficacité pour ce métier.

Des tarifs préférentiels pour les adhérents du GHR

Le partenariat entre Blockproof et le GHR prévoit tout d'abord une collaboration technique sur le RGPD avec un échange d'informations spécifiques au secteur HCR (notamment pour le blog dédié au RGPD de Blockproof).

Deux offres sont proposées, toutes deux proposant un **accès illimité à la solution numérique**.

Offre Standard	**Offre Sérénité**
Diagnostic RGPD Diagnostic de votre conformité	**Diagnostic RGPD** Diagnostic de votre conformité
2h de Formation/Atelier RGPD Enjeux RGPD pour l'hôtellerie et la restauration Démarrage de votre registre avec un expert	**2h de Formation/Atelier RGPD** Enjeux RGPD pour l'hôtellerie et la restauration Démarrage de votre registre avec un expert
Logiciel Blockproof RGPD en illimité Création de votre Registre automatisé Bibliothèque de modèles juridiques (mentions d'informations, consentement, clauses contrats salariés, CGV clients, prestataires...)	**Logiciel Blockproof RGPD en illimité** Création de votre Registre automatisé Bibliothèque de modèles juridiques (mentions d'informations, consentement, clauses contrats salariés, CGV clients, prestataires...)
	Accompagnement/suivi par Expert Vérification de votre Registre par un expert RGPD(2h) Un juriste RGPD répond à vos questions Accès FAQ
	Diagnostic annuel & maintenance

A noter : **Blockproof propose également des tarifs préférentiels exclusifs pour les adhérents du GHR** :

- jusqu'à -54% pour un hôtel ;
- jusqu'à -60% pour un restaurant.

Ces tarifs sont accessibles sur simple envoi mail de l'attestation d'adhésion au GHR au moment de la souscription. N'hésitez pas à solliciter directement Blockproof pour toutes questions ou remarques à l'adresse contact@blockproof.fr . Retrouvez ici la page du Partenaire Blockproof et ses Actualités !

4 rue de Gramont 75002 PARIS
T 01.42.96.60.75

Présentation du Département Europe et numérique

Le GHR dispose d'un Département spécialisé dans la veille réglementaire européenne et l'économie numérique depuis près d'une dizaine d'années. Ce Département dispose d'une gamme de service très large aux adhérents.

Assistance

- **Médiation exclusive** avec Booking.com, Expedia, Agoda, The Fork et Tripadvisor.
- Guide d'utilisation des plateformes numériques.

Accompagnement, conseils et informations

- Les bonnes pratiques de commercialisation sur Internet ;
- Propriété intellectuelle en ligne (marques) ;
- Cybersécurité ;
- Le choix de prestataires de solutions numériques et technologiques, notamment via la plateforme www.MonParcNum.fr ;
- La réglementation européenne et ses impacts en France.

Retrouvez tous les articles publiés par ce Département sur le site du GHR-Synhorcat :

- Actualités
- Plateformes en ligne
- Economie collaborative
- Innovation et digitalisation
- Informatique
- Europe

Pour toute demande d'information et tout renseignement, les adhérents peuvent contacter Véronique MARTENS,
Directrice du Département Europe et Numérique
v.martens@ghr.fr

Le GHR

Le Groupement des Hôtelleries & Restaurations de France (GHR) représente des établissements indépendants et sous enseigne de 5 métiers :

15000 entreprises adhérentes

130 000 salariés Soit 35% du secteur

8 commissions techniques pour accompagner les établissements au quotidien :

- Affaires sociales
- Emploi Formation
- Juridique, Economique et Fiscale
- Europe et International
- Enjeux numériques
- RSE et Sécurité Alimentaire
- Saisonniers
- Prestige, Tourisme et Promotion

Contacts

www.ghr.fr
accueil@ghr.fr
01 42 96 60 75

4 rue de Gramont 75002 PARIS
T 01.42.96.60.75