CNEC

CONSEIL NATIONAL
DES ENTREPRISES
DE COIFFURE

LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Mise en conformité des TPE/PME

EDITO

Depuis son entrée en vigueur le 25 mai 2018, le Règlement Général sur la Protection des Données étend les droits et protections des personnes concernées par des traitements de données personnelles, et impose ainsi de nouvelles obligations aux entreprises.

L'impact de ce règlement européen est considérable, dès lors qu'il s'applique à toutes les entreprises européennes et à toute entreprise internationale traitant avec des citoyens européens qui collectent des données personnelles. Peu importe le nombre de salariés, une TPE/PME est nécessairement amenée à collecter des noms, des adresses, des numéros de téléphone, des données bancaires, considérés comme des données personnelles.

Les TPE/PME qui collectent et exploitent des données personnelles -soit la quasi-totalité d'entre elles à des degrés divers- doivent ainsi entrer en conformité avec le RGPD, sous peine de lourdes sanctions financières.

Deux axes doivent ainsi être suivis à l'avenir par les TPE/PME pour se mettre en conformité avec ce nouveau règlement :

- Assurer la protection des données personnelles, et
- Être en mesure de démontrer l'effectivité de cette protection.

Ce guide a pour objet de vous présenter les principales dispositions de ce règlement, et les conséquences qu'elles ont sur votre activité. Il se veut avant tout didactique et accessible, et a pour vocation de présenter de façon pratique et concrète son impact sur votre activité.

Grâce à ce guide, vous saurez prendre des dispositions simples permettant de garantir le respect du règlement, et vous aurez en main tous les outils nécessaires afin d'assurer la sécurité de vos clients et de vos salariés, et de maintenir leur confiance.

Pierre Martin

Président de la CNAMS

SOMMAIRE

I. DÉFINITIONS

Données à caractère personnel

Toute information se rapportant à une personne physique identifiée ou identifiable (= peut être identifiée à l'aide d'un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou des éléments propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.)

Exemples : photo d'identité, coordonnées bancaires, mot de passe internet, adresse courriel, etc.

Donnée sensible

Donnée personnelle qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques ou biométriques, les données concernant la santé ou la vie et l'orientation sexuelle.
Sauf disposition légale expresse, leur collecte est interdite.

Exemple d'autorisation : les données de santé peuvent être recueillies lorsque la sauvegarde de l'intérêt vital de la personne est engagée.

Responsable de traitement

La personne qui détermine les finalités et les moyens du traitement des données personnelles.

Sous-traitant

L'organisme qui traite des données à caractère personnel pour le compte du responsable de traitement.

Traitement de données personnelles

Toute opération appliquée à des données à caractère personnel, telle que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la diffusion, etc.

II. LES NOUVELLES OBLIGATIONS DES TPE/PME EN MATIÈRE DE DONNÉES PERSONNELLES

A - CONSENTEMENT : LA COLLECTE DES DONNÉES PERSONNELLES

Votre TPE/PME est soumise à des obligations renforcées liées à l'information de la personne dont les données personnelles vont être collectées.

La personne concernée doit donc recevoir une **information complète** et exprimer un **consentement clair et explicite,** de sorte que le silence de la personne ou son absence d'opposition ne peut valoir consentement de sa part.

Afin d'être considérée comme ayant donné son consentement de manière libre et éclairée, la personne concernée doit être informée de plusieurs points :

LA FINALITÉ DE LA COLLECTE DE DONNÉES

Exemple : Informer le client que ses coordonnées bancaires doivent être collectées afin d'effectuer un prélèvement.

Exemple : Informer le client que la collecte de données est fondée :

- Sur le contrat (dans le contrat que vous aurez fait signer, il sera indiqué que le client accepte de fournir ses coordonnées bancaires afin de procéder au paiement par exemple).

- Sur l'intérêt légitime de l'entreprise (il peut ainsi être indiqué que les informations relatives à la nature des prestations choisies par le client seront conservées à des fins de statistiques).

LES PERSONNES QUI AURONT ACCÈS A SES DONNÉES

Exemple : Le salarié afin de dresser une facture, à l'exclusion de toute autre personne.

LA DURÉE DE CONSERVATION

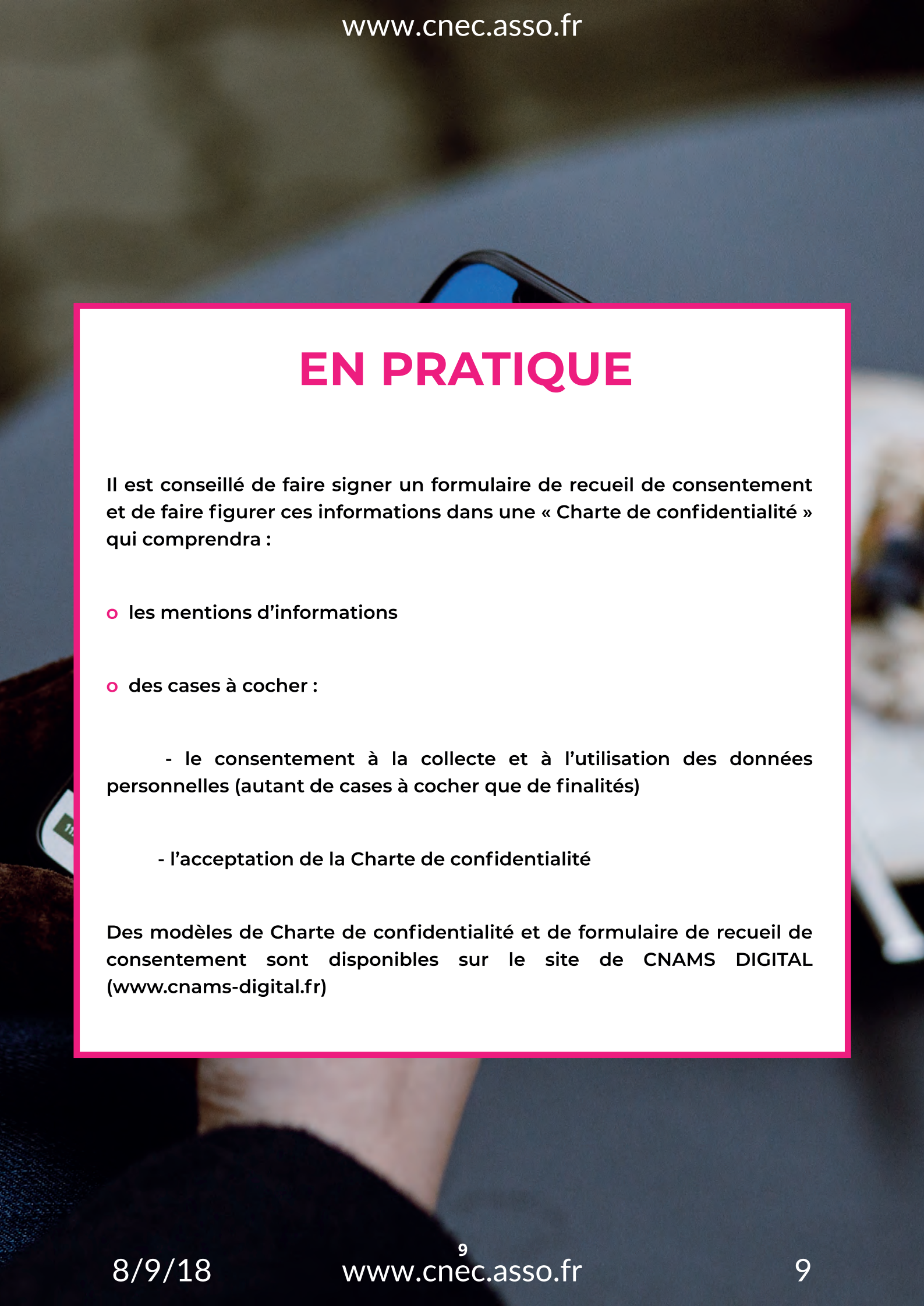
Exemple : Cinq ans après la fin de la relation contractuelle

LES MODALITÉS D'EXERCICE DES DROITS DE LA PERSONNE

Exemple : Rectification possible par e-mail ou voie postale, possibilité de s'opposer à tout moment à l'utilisation de ses données, possibilité de demander la suppression des données, etc.

L'ÉVENTUEL TRANSFERT DES DONNÉES HORS DE L'UE

Nécessité d'indiquer le pays et l'encadrement juridique qui maintiendra la protection des données.



EN PRATIQUE

Il est conseillé de faire signer un formulaire de recueil de consentement et de faire figurer ces informations dans une « Charte de confidentialité » qui comprendra :

- les mentions d'informations

- des cases à cocher :

  - le consentement à la collecte et à l'utilisation des données personnelles (autant de cases à cocher que de finalités)

  - l'acceptation de la Charte de confidentialité

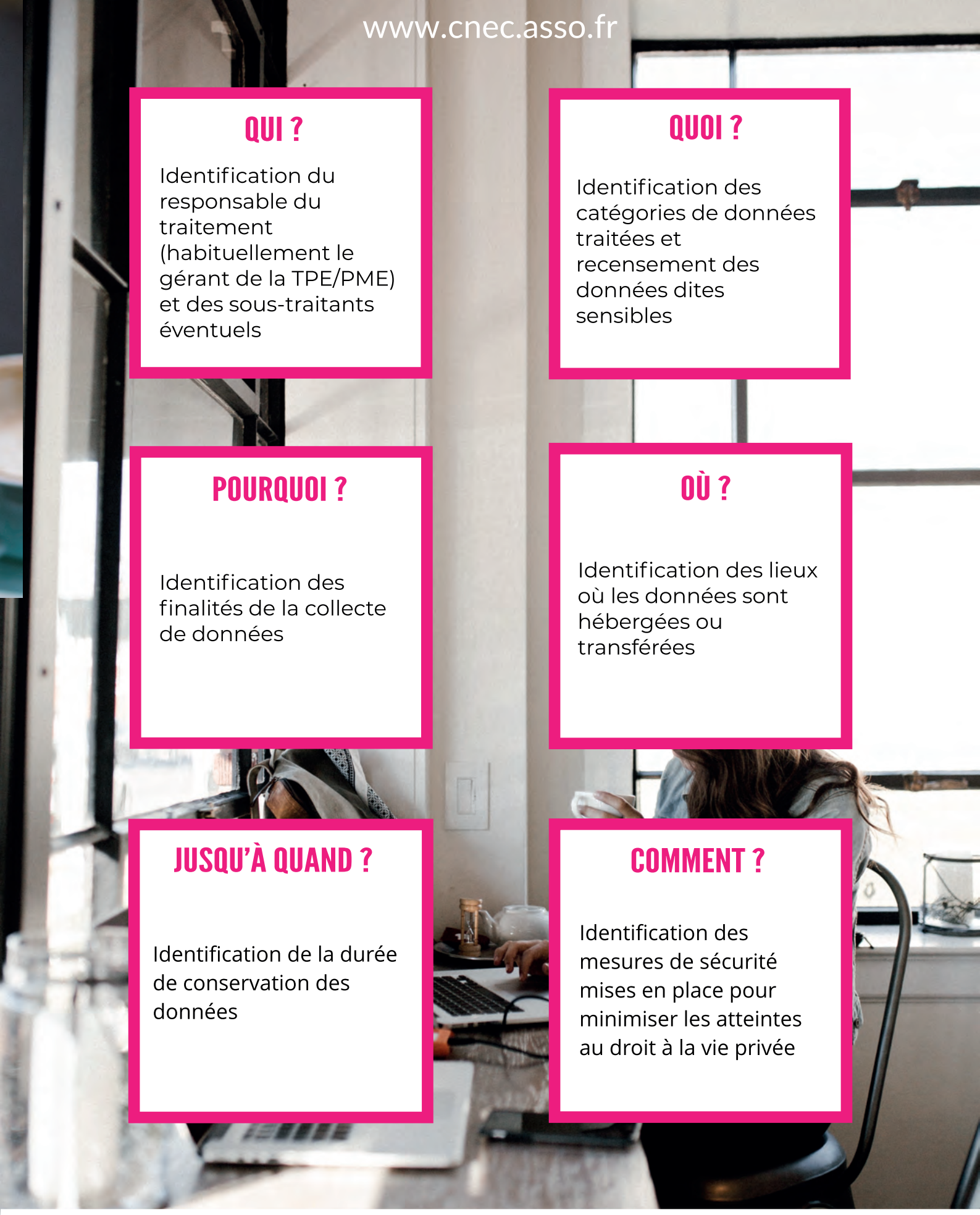
Des modèles de Charte de confidentialité et de formulaire de recueil de consentement sont disponibles sur le site de CNAMS DIGITAL (www.cnams-digital.fr)

B - LA GESTION : QUE FAIRE DES DONNÉES COLLECTÉES ?

En vertu du RGPD, l'entreprise doit être capable d'**assurer une protection** de l'intégrité des données personnelles collectées, et de **démontrer cette protection**.

La TPE/PME doit donc régulièrement procéder à un **recensement des traitements de données** afin d'être en mesure de le communiquer aux autorités de contrôle, et est tenue de garantir une certaine **sécurité** dans la conservation des données. Le RGPD confère également de **nouveaux droits** aux personnes concernées quant à leurs données personnelles et prévoit des obligations particulières à l'égard des **sous-traitants**.

La TPE/PME doit recenser au moyen de fiches les différents traitements en étant capable d'identifier les informations suivantes au sujet de chaque traitement de données :



QUI ?

Identification du responsable du traitement (habituellement le gérant de la TPE/PME) et des sous-traitants éventuels

QUOI ?

Identification des catégories de données traitées et recensement des données dites sensibles

POURQUOI ?

Identification des finalités de la collecte de données

OÙ ?

Identification des lieux où les données sont hébergées ou transférées

JUSQU'À QUAND ?

Identification de la durée de conservation des données

COMMENT ?

Identification des mesures de sécurité mises en place pour minimiser les atteintes au droit à la vie privée

Ces fiches seront réunies dans un REGISTRE DES TRAITEMENTS (pour un modèle, voir : www.cnams-digital.fr), qui devra être constamment à jour et mis à disposition de la CNIL en cas de contrôle.

EN PRATIQUE

Existe-t-il des exceptions pour les TPE/PME ?

Principe : obligation de tenir un registre des traitements.

Exception : L'obligation de tenir un registre des traitements ne s'applique pas à une entreprise ou une organisation de moins de 250 salariés.

SAUF :

- Si le traitement est susceptible de comporter un risque d'atteinte aux droits et libertés des personnes concernées.

OU

- Si le traitement de données n'est pas occasionnel (= n'est pas réalisé de manière régulière et intervient en-dehors du cours normal des activités du responsable de traitement).

OU

- Si les données collectées sont les suivantes :

  - Données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, données génétiques, données biométriques aux fins d'identifier une personne physique de manière unique, données concernant la santé ou données concernant la vie sexuelle ou l'orientation sexuelle d'une personne.
  - Données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.

Concernant l'information et les droits des personnes concernées, le recueil du consentement et l'obligation de vigilance et de sécurité du responsable de traitement, il n'existe aucune exception.

LA FINALITÉ DE LA COLLECTE DE DONNÉES

Une fois que vous aurez recensé vos données, il sera nécessaire de contrôler :

1. Que la collecte est nécessaire

Exemple : vous dirigez une entreprise de carrosserie.

Données nécessaires :

Coordonnées postales, numéro d'immatriculation, copie de la carte grise, etc.

Données non nécessaires :

Numéro de sécurité sociale, copie du permis de conduire, garage visité précédemment, etc.

2. Que les données ne sont pas "sensibles"

Exemple : en principe, la TPE/PME ne peut chercher à connaître l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques ou biométriques, les données concernant la santé ou la vie et l'orientation sexuelle du client.

3. Que l'accès aux données est limité aux personnes habilitées

Exemple : un salarié ne peut accéder librement aux informations personnelles d'un client.

Pour s'en assurer, il est possible de :

- limiter l'accès à un dossier informatique concernant les données personnelles des clients aux seules personnes habilitées au moyen d'un mot de passe permettant l'accès ;
- faire signer un engagement aux personnes habilitées reconnaissant la confidentialité des données collectées (modèle d'engagement disponible sur **www.cnams-digital.fr**).

4. Que la durée de conservation est limitée au strict nécessaire

La durée de conservation des données varie selon leur nature et sera fixée par le responsable du fichier en fonction des objectifs poursuivis.

Une fois l'objectif atteint, les données doivent être supprimées, anonymisées ou archivées (lorsque leur conservation est obligatoire).

Exemples :

- **Données de vidéosurveillance :** 1 mois maximum
- **Données relatives à la gestion de la paie des salariés :** 5 ans maximum
- **Données relatives à la carte bancaire lors d'un achat :** conservation uniquement le temps de la réalisation de l'opération de paiement.

Lorsque vous aurez effectué ces vérifications, les données qui ne sont pas régulières au regard des critères de conformité devront être effacées (pour les données non nécessaires, les données sensibles, ou les données dont la durée de conservation est excessive), ou bien leur accès devra faire l'objet d'un aménagement.

EN PRATIQUE

Que faire des données dont je dispose déjà ?

- **Données des clients (adresse, tel, coordonnées bancaires, etc.)**

Il sera simplement nécessaire de réviser les mentions d'information si besoin, d'informer les clients de leurs droits quant aux données personnelles déjà collectées, et de recueillir leur consentement pour l'avenir.

- **Données des salariés**

Dois-je solliciter les personnes et obtenir leur consentement ? Dois-je effacer les données ? Lesquelles ?

Lorsque les données sont collectées en vertu d'un contrat de travail -sous réserve de l'absence de collecte de données sensibles qui sont prohibées-, il n'est pas nécessaire de recueillir le consentement du salarié pour la collecte de ses données personnelles. Par conséquent, pour les données dont vous disposez déjà, il n'est pas nécessaire de solliciter le consentement des salariés.

En revanche, cela ne dispense pas de :

- Contrôler la conformité des données (finalités, durée de conservation, etc) ;

- Garantir les droits du salarié quant à ses données et l'informer à ce sujet ;

- D'effacer ou archiver les données lorsque leur durée de conservation est expirée (à la fin du contrat de travail par exemple).

C - LA CONSERVATION : COMMENT ET COMBIEN DE TEMPS CONSERVER LES DONNÉES COLLECTÉES ?

- LA SÉCURITÉ DES DONNÉES

Au-delà de la gestion des données, votre TPE/PME doit veiller à la sécurité de ces données en anticipant les violations éventuelles, et en réagissant en cas de violation.

- Anticipation :

La TPE/PME qui collecte les données doit prendre les mesures nécessaires afin de garantir l'intégrité des données contre les risques de diffusion ou de piratage.

Exemple : mises à jour régulières de logiciels antivirus, chiffrement des données, changement régulier de mots de passe (tous les 3 mois), etc.

- Réaction en cas de violation :

En cas de difficulté (données piratées, détruites, divulguées, etc), la TPE/PME se doit de le notifier à la CNIL (**www.cnil.fr**) dans les 72 heures suivant la violation.

Il convient également de signaler aussitôt à la personne concernée si celle-ci court un risque quant à ses données (par exemple, si un mot de passe permettant l'accès à un profil sur le site de la TPE/PME n'est plus protégé, ou s'il a pu être accédé frauduleusement à ses données personnelles).

- LE RESPECT DES DROITS DES PERSONNES DONT LES DONNÉES ONT ÉTÉ COLLECTÉES

Les personnes dont les données ont été collectées disposent de différents droits à leur égard.

La TPE/PME doit activement assurer le respect de ces droits en fournissant un accès simple et clair à chacun d'entre eux (par e-mail ou voie postale par exemple).

Les droits que vous devez garantir sont les suivants :

- DROIT D'ACCÈS

Chaque individu doit pouvoir connaître les informations que la TPE détient à son sujet.

- DROIT À LA PORTABILITÉ

Lorsque l'individu fait valoir son droit d'accès, la TPE doit lui fournir ses données personnelles dans un format "*structuré, couramment utilisé et lisible par machine*".

- DROIT À L'OUBLI (= DÉRÉFÉRENCEMENT)

Chaque individu peut demander à la TPE l'effacement de ses données personnelles. Celui-ci lui est dû dans les meilleurs délais.

- DROIT D'OPPOSITION

Chaque individu peut s'opposer à tout moment au traitement de ses données.

- LA DISPARITION DES DONNNÉES

La conservation des données personnelles est impérativement limitée dans sa durée. Cette durée est définie comme la **durée nécessaire à l'accomplissement de l'objectif poursuivi** par la collecte et le traitement.

Les données qui ne présentent plus d'intérêt pour la finalité qu'elles poursuivaient doivent donc être impérativement supprimées.

Exemple : les coordonnées de carte bancaire d'un client ne seront conservées que le temps de la réalisation de l'opération de paiement.

Certaines données doivent cependant être obligatoirement archivées.

Exemple : les données permettant de faire valoir un droit en justice doivent être conservées jusqu'à prescription de l'action en justice.

III. LE CAS DES SOUS-TRAITANTS

DE NOUVELLES OBLIGATIONS

Le RGPD met de nouvelles obligations à la charge des sous-traitants que les TPE/PME sont susceptibles d'avoir mandatés pour traiter les données personnelles collectées :

· Un sous-traitant ne peut recruter un autre sous-traitant sans l'autorisation écrite préalable du responsable de traitement ;

· Le traitement de données effectué par un sous-traitant doit être régi par un contrat ;

o **Le sous-traitant doit garantir la sécurité et la confidentialité des données** et la conformité du traitement au RGPD en conseillant son client dans la mise en conformité au RGPD ;

o **Le sous-traitant doit tenir un registre des activités de traitement effectuées** et nommer un délégué en tant que responsable de traitement.

DISPOSITIONS À PRENDRE PAR LES TPE/PME

o **Lettre avec AR à tous les sous-traitants** leur réclamant les mesures techniques et organisationnelles mises en œuvre pour assurer leur conformité au RGPD (modèle disponible sur le site suivant : **www.cnams-digital.fr**).

o **Amendement des contrats de sous-traitance** pour une mise en conformité avec le RGPD.

EN PRATIQUE

J'utilise un logiciel pour ma comptabilité et la paie. Le RGPD a-t-il un impact ?

⇨ **OUI**

Il est obligatoire pour l'employeur :

- **D'informer les salariés quant à la collecte de ces données (sur la finalité notamment) et de recueillir leur consentement.**
- **D'assurer la sécurité et la confidentialité des données durant tout leur traitement.**

C'est pour ces raisons qu'il est indispensable de contrôler les logiciels de gestion de paye utilisés par la TPE/PME :

- **Le logiciel a-t-il intégré les nouveaux principes de protection des données ?**
- **La sécurité des données est-elle techniquement assurée ?**
- **Le logiciel permet-il de prendre en compte les droits de la personne concernée (droit à l'effacement par exemple) ?**

Il est recommandé de contacter les éditeurs des logiciels afin de négocier les contrats avec eux.

IV. SYNTHÈSE

Afin de certifier la conformité au RGPD, la TPE/PME doit s'assurer :

- De la bonne tenue du registre des traitements ;
- De l'exhaustivité des informations transmises aux personnes concernées ;
- De détenir la preuve du consentement libre, éclairé et explicite des personnes concernées ;
- Du respect des délais de conservation des données personnelles ;
- De la mise en place de mesures de sécurité pour protéger l'intégrité des données ;
- De garantir le respect des droits des personnes.

EXEMPLE 1

JE DIRIGE UN SALON DE COIFFURE QUI EMPLOIE DEUX SALARIÉS ET UN APPRENTI.

J'UTILISE UN LOGICIEL DE PAIE ET UN LOGICIEL DE PRISE DE RENDEZ-VOUS ET DE CRM (GESTION DE LA RELATION CLIENT)

DONNÉES PERSONNELLES COLLECTÉES :

Je recueille des données :

- des salariés :
Adresse, numéro de téléphone, situation familiale, permis de conduire, etc.

- des clients :
Coordonnées postales, coordonnées bancaires, etc

AFIN D'ASSURER LA MISE EN CONFORMITÉ DE MA TPE AVEC LE RGPD :

1 - J'édite une Charte de confidentialité faisant mention de toutes les informations obligatoirement transmise aux personnes concernées ;

=> Pour un modèle, voir : **www.cnams-digital.fr**

2 - Je m'assure de la conformité au RGPD du formulaire de collecte qui permettra de recueillir un consentement clair et explicite ;

=> Pour un modèle de formulaire, voir : **www.cnams-digital.fr**

3 - Au moyen de fiches, je recense et contrôle les traitements de données déjà en place dans la TPE ;

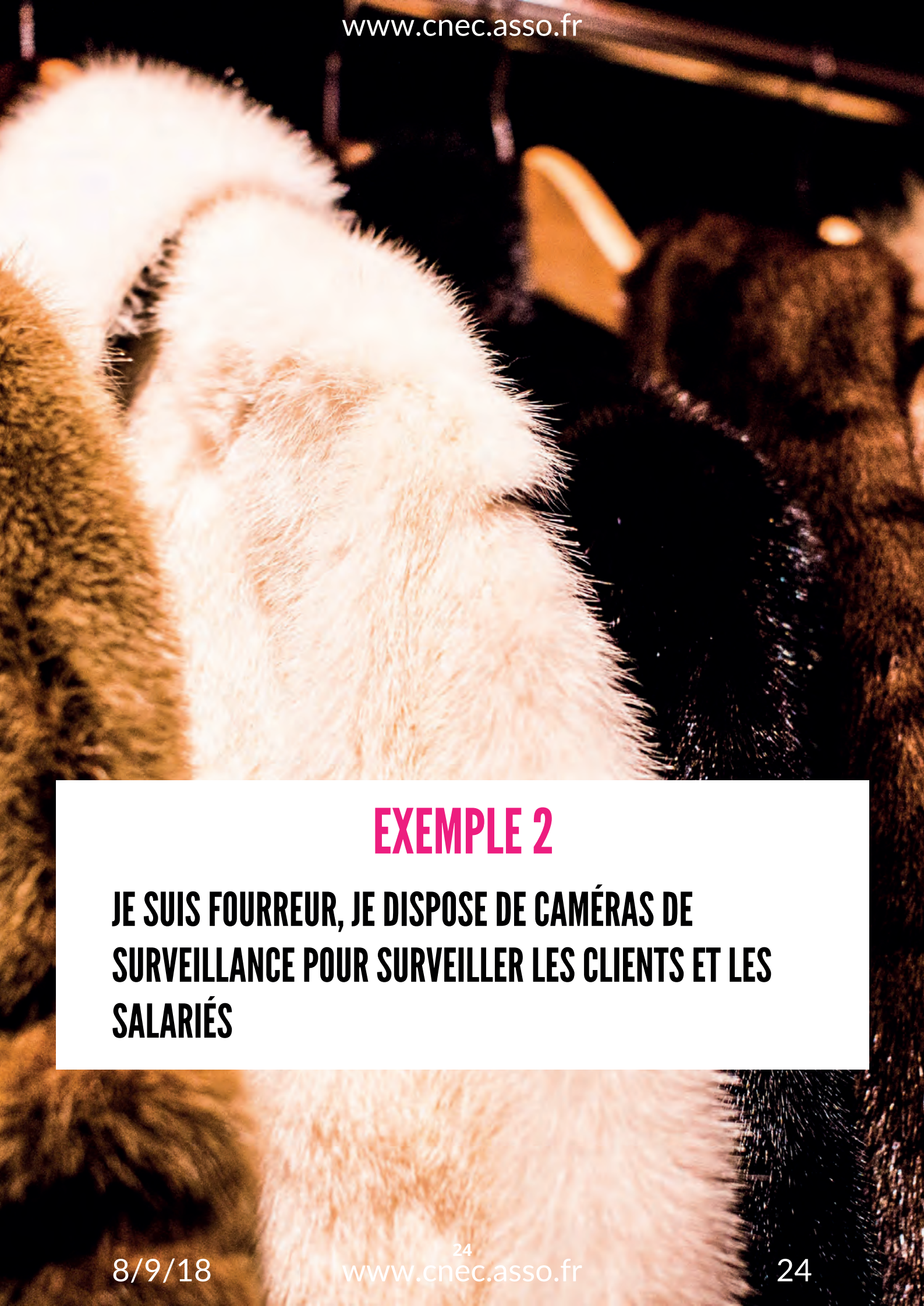
4 - J'efface les données déjà collectées qui sont illégales au regard du RGPD.

Concernant les données qui ne sont pas illégales mais qui ne sont pas en conformité avec le RGPD, je les régularise (ex : accès aux personnes habilitées, recueil du consentement, etc)

5 - Je m'assure que les droits des personnes quant à l'accès, au déréférencement, à la portabilité et l'opposition sont effectivement garantis ;

6 - Je m'assure que les logiciels de traitement des données permettent de conserver ces données en sécurité ; si ce sont des dossiers « papier », je m'assure de leur confidentialité et de la limitation de leur accès (personnes habilitées, utilisation d'un coffre, etc) ;

7 – Dès maintenant, je rentre en contact avec mes éventuels sous-traitants (par exemple l'éditeur du logiciel de paie) afin de vérifier leur conformité avec le RGPD.



EXEMPLE 2

JE SUIS FOURREUR, JE DISPOSE DE CAMÉRAS DE SURVEILLANCE POUR SURVEILLER LES CLIENTS ET LES SALARIÉS

DONNÉES PERSONNELLES COLLECTÉES :

Coordonnées postales et bancaires des clients, images de vidéosurveillance, etc.

AFIN D'ASSURER LA CONFORMITÉ DE MA TPE AVEC LE RGPD :

1 – Je pose un panneau visible indiquant la présence de caméras de surveillance.

Attention :

- **Les caméras ne doivent pas filmer les employés sur leur poste de travail,** sauf circonstances particulières (employé manipulant de l'argent par exemple, mais la caméra doit davantage filmer la caisse que le caissier) ;
- **Les caméras ne doivent pas filmer les zones de pause** ou de repos des employés, ni les toilettes ;

2 - J'édite une Charte de confidentialité faisant mention de toutes les informations que doivent connaître les personnes concernées et que je fais signer dès qu'un client me transmet ses données ;

3 - Je m'assure de la conformité au RGPD du formulaire de collecte qui permettra de recueillir un consentement clair et explicite ;

4 - Au moyen de fiches, **je recense et contrôle les traitements de données** déjà en place dans la TPE ;

5 - J'efface les données déjà collectées qui ne me semblent pas en conformité avec le RGPD. ;

6 - Je m'assure que les droits des personnes quant à l'accès, le déréférencement, la portabilité et l'opposition sont effectivement garantis ;

7 - Je m'assure que les logiciels de traitement des données permettent de conserver ces données en sécurité. Je vérifie notamment que les logiciels de traitement des images de vidéosurveillance sont sécurisés et à jour du RGPD. Dans le doute, je contacte l'entreprise proposant le service de vidéosurveillance afin de contrôler la mise en conformité et négocier le contrat le cas échéant ;

8 – Dès maintenant, **je rentre en contact avec les éventuels sous-traitants** (si la vidéosurveillance est traitée par une entreprise tierce par exemple) afin de vérifier leur conformité avec le RGPD.

EXEMPLE 3

JE SUIS RESPONSABLE D'UN SALON DE TOILETTAGE POUR CHIENS ET J'ACCUEILLE UN STAGIAIRE

DONNÉES PERSONNELLES COLLECTÉES :

Coordonnées postales et bancaires des clients et du stagiaire, etc.

AFIN D'ASSURER LA CONFORMITÉ DE MA TPE AVEC LE RGPD :

1 – Si mon stagiaire a entre 13 et 15 ans, **je me charge d'obtenir le consentement parental pour chaque traitement de données personnelles**. J'utilise tous les moyens possibles pour m'assurer que la personne qui donne le consentement est bien titulaire de l'autorité parentale ;

2 - J'édite une Charte de confidentialité faisant mention de toutes les informations que doivent connaître les personnes concernées. Je m'assure que le langage employé est accessible à mon jeune stagiaire ;

3 - Je m'assure de la conformité au RGPD du formulaire de collecte qui permettra de recueillir un consentement clair et explicite ;
3 - Au moyen de fiches, **je recense et contrôle les traitements de données** déjà en place dans la TPE ;

4 - J'efface les données déjà collectées qui ne me semblent pas en conformité avec le RGPD ;

5 - Je m'assure que les droits des personnes quant à l'accès, le déréférencement, la portabilité et l'opposition sont effectivement garantis. Si mon stagiaire demande à exercer un de ces droits, je veille à recourir à une procédure accélérée et j'accède à sa demande en moins d'un mois ;

6 - Je m'assure que les logiciels de traitement des données permettent de conserver ces données en sécurité ;

7 – Dès maintenant, **je rentre en contact avec les éventuels sous-traitants** afin de vérifier leur conformité avec le RGPD.

www.cnams-digital.fr

La première plateforme dédiée à la digitalisation des entreprises du secteur de l'artisanat des métiers de service et de fabrication.

CNEC

CONSEIL NATIONAL
DES ENTREPRISES
DE COIFFURE