FICHE TECHNIQUE

Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel entrera en vigueur le 25 mai 2018[1].

D'application directe, il devrait néanmoins être complété dans les prochains mois par une loi française qui l'intègrerait à la loi « Informatique et libertés » de 1978, pour en faciliter la lisibilité[2].

Les offices de tourisme sont directement concernés par cette règlementation car ils sont très souvent responsables de « traitements automatisés de données à caractère personnel », c'est-à-dire en pratique, de fichiers, de sites internet ou de bases de données regroupant des informations variées sur leurs clients, prospects, usagers, salariés etc. (noms, adresses, dates de naissances etc.) dont ils font parfois usage dans leurs systèmes de réservation, pour l'envoi de newsletters voire de sollicitations commerciales ciblées. A noter que la règlementation vise aussi bien les traitements informatiques que les traitements dits « papier » (par exemple, la saisie manuscrite d'un registre).

Compte-tenu de la diversité des situations, tant au niveau des formes juridiques des offices de tourisme que des types de traitement utilisés, la présente fiche ne prétend pas à l'exhaustivité et ne peut remplacer une consultation d'avocat. Elle a plutôt pour ambition de résumer les principales innovations règlementaires (1) et de vous orienter vers la documentation utile à la préparation de cette transition (2).

1) Un aperçu des évolutions à intervenir

Le règlement a trois objectifs principaux[3] :

- Renforcer les droits des personnes ;
- Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;
- Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données en Europe.

Ce sont les deux premiers objectifs qui nous occuperont ici car plus proches des réalités quotidiennes des offices de tourisme.

[1] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679
[2] http://www.assemblee-nationale.fr/15/dossiers/donnees_personnelles_protection.asp
[3] https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

a) Les droits des personnes concernées

Le consentement :
En principe, le responsable d'un traitement doit obtenir le consentement de la personne concernée pour récolter ses données personnelles (sauf nécessité liée à l'exécution d'une mission de service public). Ce consentement est désormais défini et nécessitera la mise à disposition préalable d'une information claire, intelligible et aisément accessible sur l'usage qui en sera fait par le responsable de traitement. En pratique, les mentions d'information devront être précisées et il restera nécessaire pour le professionnel de conserver la preuve du consentement, matérialisé de façon non ambigüe (case à cocher non pré-remplie accompagnée d'une mention d'acceptation, par exemple).

Pour les mineurs de moins de 16 ans, l'information sur le traitement devra être rédigée en des termes clairs et simples que l'enfant peut aisément comprendre. En revanche, c'est auprès du représentant légal (parent), qu'il faudra obtenir le consentement. Attention donc aux jeux à destination des moins de 16 ans, permettant la récolte de leurs informations lors de l'inscription. A l'âge adulte, le consentement donné peut être retiré et les données effacées.

Le droit d'opposition :
Que le consentement ait été ou non recueilli préalablement, la personne concernée conserve un droit d'opposition à l'utilisation de ses données. Pour faire valoir ce droit, elle doit désormais obligatoirement avoir à sa disposition une adresse mail et non plus simplement une adresse postale. Il s'agit en pratique d'effacer et de déréférencer les données concernées. Il conviendra également de prévoir un système supprimant automatiquement les données à l'issue de la période de conservation (durée variable selon le traitement en question).

La portabilité :
Il s'agit d'un nouveau droit de récupérer les données collectées sous une forme aisément réutilisable pour les transmettre à un tiers.

Actions collectives :
Comme en matière de consommation, les associations pourront introduire des recours collectifs en matière de protection des données.

Droit à réparation :
Toute personne ayant subi un dommage matériel ou moral du fait de la violation de la règlementation pourra obtenir une indemnisation du préjudice subi.

b) Obligations des responsables de traitement

Allègement des formalités administratives et études d'impact[4] :
En contrepartie de l'allègement des formalités administratives (déclaration, autorisation), le responsable de traitement et ses sous-traitants (prestataires informatiques, par exemple), sont grandement responsabilisés.

Lorsque les traitements ne constituent pas un risque pour la vie privée des personnes, il n'y aura plus d'obligation de déclaration.

Toute la subtilité sera d'apprécier s'il existe ou non un risque pour la vie privée des personnes car il conviendra, en présence d'un tel risque, de faire réaliser une étude d'impact.

En pratique, la CNIL indique que les traitements concernés sont ceux comportant des données sensibles (origine ethnique, opinions politiques, philosophiques ou religieuses, appartenance syndicale, santé, orientation sexuelle, données génétiques).

A priori, les offices ne devraient pas être concernés par de telles données. Néanmoins, la pratique du profilage, c'est-à-dire « l'évaluation systématique et approfondie d'aspects personnels des personnes physiques », qui se pratique régulièrement en matière touristique, sera désormais considérée comme sensible. Attention donc à la nécessité de réaliser cette étude d'impact, à l'aide si besoin, du délégué à la protection des données.

Le délégué à la protection des données (DPO, *Data Protection Officer*) :
Sa désignation est obligatoire dans toute structure publique. Semblent donc directement concernés les offices exerçant sous forme de régie ou d'EPIC.

Pour les associations, il n'y aurait donc pas d'obligation a priori mais la désignation de ce délégué est tout de même vivement recommandée par la CNIL compte tenu des nombreuses obligations qui reposent sur la structure en cette matière.

La désignation du DPO est également obligatoire si les activités de la structure l'amène à « réaliser un suivi régulier et systématique des personnes à grande échelle », ou à traiter des données sensibles, toujours à grande échelle (notion qui laisse place à l'interprétation…).

Le délégué sera chargé d'informer et de conseiller la structure et ses employés, de contrôler le respect du règlement, de conseiller la structure sur la réalisation d'une analyse d'impact, de coopérer avec la CNIL.

Il s'agit en quelque sorte du successeur du CIL, Correspondant Informatique et Libertés, poste déjà créé dans plusieurs CRT, CDT et OT[5]. Comme on le verra ci-après, la désignation

[4] https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil
[5] https://www.data.gouv.fr/fr/datasets/correspondants-informatique-et-libertes-cil/

d'un CIL dès aujourd'hui selon les règles actuelles peut être un bon moyen d'anticiper l'entrée en vigueur du nouveau règlement.

Principe de minimisation :
Seules les données strictement nécessaires au traitement doivent être récoltées ; par exemple, il est inutile de connaître le nom d'une personne s'il s'agit uniquement de réaliser des statistiques de fréquentation.

En pratique, il conviendra d'éviter sur les formulaires d'inscription en ligne les « champs libres » où les contacts sont amenés à choisir librement les informations données. Il convient plutôt de les guider au moyen de listes préétablies permettant de vérifier que les données collectées servent la finalité du traitement.

Mesures de protection appropriées d'un point de vue technique et démonstration de conformité :
Toujours en contrepartie de l'allègement des formalités administratives, il s'agira non seulement de mettre en place des mesures techniques et organisationnelles de protection mais également d'être en mesure de démontrer la conformité de ces mesures à l'aide d'une documentation appropriée (registre de traitement, études d'impact, modèles de mentions d'informations, modèles de formulaire de recueil du consentement, contrats avec les sous-traitants etc.).

Pour plus de précisions, on renverra aux documents disponibles sur le site de la CNIL[6] et aux prestataires techniques spécialisés.

Notification de failles de sécurité aux autorités et personnes concernées dans les 72 heures :
Il s'agit d'une nouvelle obligation pour le responsable de traitement.

Certification de traitements :
Plusieurs normes et référentiels devraient être mis en place à l'aide de structures spécialisées.

Des codes de conduite sont également envisagés.

Sanctions :
Elles seront bien entendu graduées (avertissement, suspension du traitement, rectification) mais peuvent aller, en ce qui concerne les amendes administratives jusqu'à 10 ou 20 millions d'euros et pour une entreprise de 2 à 4 % du chiffre d'affaires mondial.

2) Comment se préparer en pratique ?

La CNIL (Commission Nationale de l'Informatique et des Libertés) propose les six étapes suivantes[7] :

[6] https://www.cnil.fr/fr/organiser-les-processus-internes
[7] https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

- Désigner un pilote : par exemple, un CIL (futur DPO, délégué à la protection des données)

- Cartographier les traitements de données personnelles : quels types de données sont collectés ? dans quels outils ? pour quelle utilisation future ? ma structure détermine-t-elle l'utilisation des données ? s'agit-il au contraire d'un traitement géré par un tiers (le CDT ou le CRT par exemple) ?

- Prioriser les actions à mener : réduire le nombre de données collectées le cas échéant, réviser les mentions d'information, prendre contact auprès des sous-traitants et renégocier les contrats, organiser les droits d'accès, mesures de sécurité etc.

- Gérer les risques : réalisation de l'analyse d'impact, le cas échéant,

- Organiser les processus internes : gestion des demandes de rectification, formation du personnel etc.

- Documenter la conformité : établir le registre des traitements, rédiger les analyses d'impact, conserver les modèles d'information, décrire les procédures mises en place, conserver les contrats, les preuves de consentement, les notifications en cas de défaillance de sécurité…

Il conviendra enfin d'être attentif à la promulgation de la loi française à intervenir qui pourrait compléter certains points, notamment quant au régime d'autorisation de certains traitements auprès de la CNIL.

Nous vous souhaitons, en guise de conclusion, beaucoup de courage dans la mise en place de ces différentes mesures et espérons que la mise en conformité se déroulera sans heurts.

B.D.D. AVOCATS
29, AVENUE GEORGES MANDEL
75116 PARIS

Elise FABING
Emmanuel WELLER
Avocats au Barreau de Paris

Sources :

- http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679
- http://www.assemblee-nationale.fr/15/dossiers/donnees_personnelles_protection.asp
- www.cnil.fr
- https://www.data.gouv.fr/fr/datasets/correspondants-informatique-et-libertes-cil/
- MATTATIA, *Revue Lamy Droit de l'Immatériel*, n°126, 1er mai 2016, Synthèse du futur règlement européen sur les données personnelles,
- http://www.tourhebdo.com/actualites/technologie/donnees-personnelles-les-3-evolutions-a-venir-du-profilage-voyageur-447062.php