Quelles sont les obligations des professionnels en matière de démarchage téléphonique ?

écrit par Marine de la Clergerie | 07/03/2025

À PROSCRIRE

 Ne pas démarcher téléphoniquement un consommateur inscrit sur BLOCTEL

 Ne pas louer, vendre, ou mettre à disposition des fichiers contenant des données téléphoniques de consommateurs inscrits sur BLOCTEL

À RESPECTER

 Souscrire un abonnement BLOCTEL : https://pro.bloctel.gouv.fr/

 Vérifier ses fichiers sur BLOCTEL :

- Au moins une fois par mois s'il exerce à titre habituel une activité de démarchage téléphonique,
- Avant toute campagne de démarchage téléphonique dans les autres cas

 Respecter les jours et horaires autorisés pour le démarchage téléphonique (sauf « consentement exprès et préalable du consommateur »)

- Du lundi au vendredi, de 10h à 13h et de 14h à 20h
- Pas les jours fériés
- Pas plus de 4 fois par mois
- En cas d'opposition lors de la conversation, le professionnel ne peut pas le rappeler avant 60 jours.

 Le professionnel peut continuer à solliciter le consommateur inscrit sur BLOCTEL si :

- Le consommateur est un client et
- La sollicitation est en rapport avec le contrat

Références

- Article L223-1 du Code de la consommation
- Article D223-9 du Code de la consommation

Actualités:

- 14.05.2025: Adoption au Sénat d'une proposition de loi contre toutes les fraudes intégrant la proposition de 2024. BLOCTEL devrait disparaître.
- 30.09.2024: Proposition de loi interdisant le démarchage téléphonique sans consentement à compter du 11 août 2026

Contact: Vous souhaitez en savoir plus sur le droit du démarcharge téléphonique en France? Contactez Marine de la Clergerie (contact@mdc-avocat.fr, www.mdc-avocat, Consultation, LinkedIn), Avocat au Barreau de Toulouse, spécialiste en Droit du numérique et des communications, avec la qualification spécifique Droit des données à caractère personnel.

La lutte contre le spoofing téléphonique

écrit par Marine de la Clergerie | 07/03/2025
Le spoofing téléphonique est une technique permettant d'usurper un numéro d'appel pour tromper le destinataire.

Les fraudeurs utilisent la méthode du « spoofing téléphonique » pour se faire passer pour une banque, un organisme public ou une entreprise, incitant les victimes à divulguer des informations sensibles ou à effectuer des virements frauduleux.

Depuis le 1er octobre 2024, les opérateurs de téléphonie français doivent lutter contre le spoofing.

Références

- Article L44 du Code des postes et des télécommunications modifié par

l'article 10 de la loi n°2020-901 du 24 juillet 2020
- MAN: Mécanisme d'Authentification des numéros

Contact: Vous avez une problématique de spoofing téléphonique? Contactez Me Marine de la Clergerie (contact@mdc-avocat.fr, www.mdc-avocat, Consultation, LinkedIn), Avocat au Barreau de Toulouse, spécialiste en Droit du numérique et des communications, avec la qualification spécifique Droit des données à caractère personnel.

DPO – Ressources utiles

écrit par Marine de la Clergerie | 07/03/2025

Actualités des DPO

- 21.01.2025 – CEDPO – In the DPO's Own Words: "Trends and Challenges beyond 2024"

FAQ DPO

- Qu'est-ce-qu'un DPO?
- Un DPO est-il obligatoire?
- Formulaire de contact – Comment analyser sa conformité au RGPD?
- L'avocat DPO

Les offres DPO

- Audit RGPD
- Hotline RGPD/DPO
- Formation DPO/RGPD
- DPO externalisé

- Support DPO interne

Les qualifications de Me de la Clergerie, Avocat & DPO

- Avocat au Barreau de Toulouse
- Spécialiste en Droit du numérique et des communications, avec la qualification spécifique Droit des données à caractère personnel
- DPO certifié (Certification VERITAS)
- Diplôme du CNAM « Certificat de spécialisation Cybersécurité et RGPD » (2024)

Contact: Besoin d'un avocat pour un problème RGPD ou DPO? contactez Me Marine de la Clergerie, Avocat & DPO (contact@mdc-avocat.fr, www.mdc-avocat, Consultation, LinkedIn). Me Marine de la Clergerie, Avocat au Barreau de Toulouse, spécialiste en Droit du numérique et des communications, avec la qualification spécifique Droit des données à caractère personnel ET DPO certifié (VERITAS), accompagne régulièrement ses clients pour des audit RGPD, lors des contrôles de la CNIL, en tant que DPO externe.

Le dispositif PERCEVAL pour les fraude à la carte bancaire

écrit par Marine de la Clergerie | 07/03/2025

Attention, avant tout signalement PERCEVAL, il faut faire opposition à la carte de paiement.

- **Comment procéder au signalement?** Le signalement se fait sur le site suivant: https://www.service-public.fr/particuliers/vosdroits/R46526

Le signalement s'effectue sur le site service-public.fr, où la victime se connecte et

s’authentifie via le dispositif FranceConnect. Elle y renseigne ses informations personnelles, les détails de la carte bancaire concernée ainsi que les circonstances de la fraude. Avant toute déclaration, il est impératif d’avoir fait opposition à la carte de paiement.

- **Quand a été créé le dispositif PERCEVAL?** Le dispositif PERCEVAL a été créé par un arrêté du 23 mai 2018.
- **A quoi sert le dispositif PERCEVAL?** Le dispositif PERCEVAL permet aux victimes d’une fraude à la carte bancaire, commise par un auteur inconnu sur internet, de la signaler.
- **Quelles sont les conditions pour utiliser le dispositif PERCEVAL?** Les signalements effectués via ce dispositif doivent répondre à deux critères : (1) L’auteur de la fraude doit être inconnu de la victime; (2) Le délit doit appartenir à la liste des infractions mentionnées à l’article L163-3 du Code monétaire et financier.
- **Quelles sont les infractions visées par le dispositif PERCEVAL?** Ces infractions comprennent :
    - La contrefaçon ou la falsification d’un instrument de paiement doté d’un dispositif de sécurité personnalisé;
    - L’usage ou la tentative d’usage, en connaissance de cause, d’un tel instrument contrefait ou falsifié;
    - L’acceptation, en connaissance de cause, d’un paiement au moyen d’un instrument contrefait ou falsifié.

Ces délits sont passibles de cinq ans d’emprisonnement et de 375 000 € d’amende, des peines alourdies lorsqu’ils sont commis par une personne morale (article 131-38 du Code pénal).

- **Que se passe-t-il après le signalement sur la plateforme PERCEVAL?** Une fois le signalement déposé sur la plateforme PERCEVAL, les services de police ou de gendarmerie peuvent initier des investigations. Ce signalement facilite également les démarches de la victime auprès de sa banque : le récépissé PERCEVAL peut être transmis dans le cadre de la procédure d’indemnisation prévue à l’article L.133-18 du Code monétaire et financier.

- **A quoi sert la plateforme PERCEVAL?** La plateforme permet d'exploiter les déclarations afin d'identifier des rapprochements et d'uniformiser les démarches administratives auprès des établissements bancaires.

Attention toutefois, un faux signalement délibéré expose son auteur à une peine de six mois d'emprisonnement et 7 500 € d'amende (article 434-26 du Code pénal).

Contact: Vous êtes victime d'une fraude à la carte bancaire? contactez Me Marine de la Clergerie (contact@mdc-avocat.fr, www.mdc-avocat, Consultation, LinkedIn), Avocat au Barreau de Toulouse, spécialiste en Droit du numérique et des communications, avec la qualification spécifique Droit des données à caractère personnel.

DPO – Comment analyser un formulaire de contact au regard du RGPD ?

écrit par Marine de la Clergerie | 07/03/2025
Vous êtes DPO et vous devez vous assurer de la conformité du formulaire de contact mis en œuvre par le responsable de traitement.

En pratique, il est nécessaire d'analyse le formulaire de collecte au regard des exigences du RGPD et en particulier :

- Des exigences de l'article 5 du RGPD (principes relatifs au traitement des données à caractère personnel) :
    - Est-ce que les données sont traitées de manière licite, loyale et transparente ?
    - Est-ce que les données sont collectées pour des finalités déterminées, explicites et légitimes ?

    - Est-ce que les données sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ?
    - Est-ce que les données sont exactes et et, si nécessaire, tenues à jour ?
    - Est-ce que la durée de conservation de ces données est déterminée et non excessive ?
    - Est-ce que les mesures de sécurité adaptées sont mises en place pour protéger ces données ?

- Des exigences de l'article 6 (licéité du traitement) :
    - Est-ce que le traitement est licite ?

- Des exigences de l'article 9 (données particulières) :
    - Le traitement ne porte pas sur des données sensibles

- Des exigences des articles 12 & 13 du RGPD (information des personnes) :
    - Est-ce que les informations ont été fournies aux personnes d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ?
    - Les informations listées à l'article 13 sont-elles fournies ?

Contact: Marine de la Clergerie (contact@mdc-avocat.fr, www.mdc-avocat, Consultation, LinkedIn), Avocat au Barreau de Toulouse & DPO, spécialiste en Droit du numérique et des communications, avec la qualification spécifique Droit des données à caractère personnel.