cnil.fr

Prospection commerciale et droits des personnes : sanction de 600 000 euros à l'encontre d'EDF

5–6 minutes

Le 24 novembre 2022, la CNIL a sanctionné la société EDF d'une amende de 600 000 euros, notamment pour ne pas avoir respecté ses obligations en matière de prospection commerciale et de droits des personnes.

Le contexte

La CNIL a reçu plusieurs plaintes concernant les difficultés rencontrées par des personnes dans la prise en compte de leurs droits par la société EDF, premier fournisseur d'électricité en France.

Sur la base des constatations effectuées lors des contrôles, la formation restreinte – organe de la CNIL chargé de prononcer les sanctions – a considéré que la société avait manqué à plusieurs obligations prévues par le règlement général sur la protection des données (RGPD) et le code des postes et des communications électroniques (CPCE). Elle a prononcé à l'encontre de la société EDF une amende de 600 000 euros rendue publique.

Le montant de cette amende a été décidé au regard des manquements retenus, ainsi qu'en tenant compte de la coopération de la société et de l'ensemble des mesures qu'elle a prises au cours de la procédure pour se mettre en conformité sur tous les manquements qui lui étaient reprochés.

Les manquements sanctionnés

Un manquement à l'obligation de recueillir le consentement des personnes à recevoir de la prospection commerciale par voie électronique (articles L. 34-5 du CPCE et 7 du RGPD)

Entre 2020 et 2021, EDF a réalisé une campagne de prospection commerciale par voie électronique. Cependant, elle n'a pas été en mesure de démontrer à la CNIL qu'elle avait obtenu au préalable un consentement valable des personnes.

Lors des contrôles, la société a fourni à la CNIL deux exemples de formulaire type de collecte de données des prospects mis à sa disposition par un courtier en données (*data broker* en anglais). Toutefois, elle n'a pas été en mesure de communiquer à la CNIL la liste

des partenaires destinataires des données, alors qu'une telle liste doit être tenue à la disposition des personnes au moment de donner leur consentement.

Enfin, les mesures mises en place par la société EDF auprès de ses courtiers en données pour s'assurer que le consentement a été valablement donné par les personnes avant d'être démarchées étaient insuffisantes. En effet, la société a reconnu qu'à la date des contrôles, elle n'exerçait aucune vérification sur les formulaires de recueil du consentement utilisés et qu'elle ne réalisait pas d'audits sur les courtiers en données.

Des manquements à l'obligation d'information (articles 13 et 14 du RGPD) et au respect de l'exercice des droits (articles 12, 15 et 21 du RGPD)

Les vérifications effectuées par la CNIL ont également permis de mettre en évidence d'autres manquements retenus dans la décision de sanction :

- Un manquement à **l'obligation d'information des personnes :** la charte de protection des données personnelles qui figurait sur le site web de la société ne précisait pas la base légale correspondant à chaque cas d'usage des données et était imprécise sur les durées de conservation (article 13 du RGPD). De plus, dans le premier courrier de prospection commerciale adressé par EDF aux personnes, la source des données n'était pas indiquée de façon suffisamment précise. EDF écrivait seulement que les « *données ont été collectées auprès d'un organisme spécialisé dans l'enrichissement de données* », sans indiquer précisément d'où provenaient les données (article 14 du RGPD).
- Un manquement aux obligations relatives aux **modalités d'exercice des droits** (article 12 du RGPD) : la société n'a notamment pas répondu à certains plaignants dans le délai d'un mois prévu par les textes.
- Un manquement à l'obligation de respecter le **droit d'accès aux données** (article 15 du RGPD) et le **droit d'opposition** des personnes concernées (article 21 du RGPD). La société a donné des informations inexactes sur la source des données collectées et n'a pas pris en compte l'opposition à recevoir de la prospection commerciale.

Un manquement à l'obligation d'assurer la sécurité des données personnelles (article 32 du RGPD)

La formation restreinte a également retenu un manquement à l'obligation d'assurer la sécurité des données personnelles puisque :

- les mots de passe d'accès à l'espace client du portail « prime énergie » de plus de 25 000 comptes étaient conservés de manière non sécurisée jusqu'à juillet 2022 ;
- les mots de passe d'accès à l'espace client EDF de plus de 2,4 millions comptes étaient uniquement hachés (une série de caractères calculés à la place du mot de passe), sans avoir été salés (ajout de caractères aléatoires avant le hachage, pour éviter de retrouver un mot de passe par comparaison de hachages), ce qui les exposait à des risques.