Délibération SAN-2022-021 du 24 novembre 2022

Commission Nationale de l'Informatique et des Libertés

Nature de la délibération : Sanction
Etat juridique : En vigueur

Date de publication sur Légifrance : Mardi 29 novembre 2022

Délibération de la formation restreinte n°SAN-2022-021 du 24 novembre 2022 concernant la société ÉLECTRICITÉ DE FRANCE

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Monsieur Alexandre LINDEN, président, Monsieur Philippe-Pierre CABOURDIN, vice-président, Monsieur Alain DRU et Monsieur Bertrand du MARAIS, membres ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ;

Vu le code des postes et des communications électroniques ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants ;

Vu le décret no 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération no 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2021-020C du 4 janvier 2021 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par la société ÉLECTRICITÉ DE FRANCE ou pour son compte ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 19 mai 2022 ;

Vu le rapport de Madame Valérie PEUGEOT, commissaire rapporteure, notifié à la société ÉLECTRICITÉ DE FRANCE le 23 juin 2022 ;

Vu les observations écrites versées par le conseil de la société ÉLECTRICITÉ DE FRANCE le 25 juillet 2022 ;

Vu la réponse de la rapporteure à ces observations notifiée le 11 août 2022 au conseil de la société ;

Vu les observations écrites versées par le conseil de la société ÉLECTRICITÉ DE FRANCE le 9 septembre 2022 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 13 octobre 2022 :

- Madame Valérie PEUGEOT, commissaire, entendue en son rapport ;

en qualité de représentants de la société ÉLECTRICITÉ DE FRANCE :

- […] ;

La société ÉLECTRICITÉ DE FRANCE ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. Créée en 1955, la société ÉLECTRICITÉ DE FRANCE (ci-après " la société EDF " ou " la société ") est une société anonyme à conseil d'administration dont le siège social est situé 22 avenue de Wagram à Paris (75008).

2. Le groupe EDF, lequel comprend la société-mère EDF et ses filiales, est principalement actif en France et à l'étranger sur les marchés de l'électricité et, en particulier, dans la production d'électricité (nucléaire, renouvelable et fossile) et la vente en gros, le négoce, le transport, la distribution et la fourniture d'électricité. Le groupe EDF est également présent sur les marchés du gaz et des services énergétiques, ainsi que dans la construction, l'exploitation et la maintenance de centrales électriques et de réseaux électriques et fournit des services de recyclage des déchets et des services énergétiques. Le groupe EDF emploie plus de 131 000 salariés, dont plus de 63 000 pour la société EDF.

3. En 2020, le groupe EDF a réalisé un chiffre d'affaires de plus de 69 milliards d'euros pour un résultat net de […] euros. En 2021, son chiffre d'affaires s'est élevé à plus de 84 milliards d'euros pour un résultat net de […] euros.

4. Dans le cadre des services fournis par la société, des données à caractère personnel de ses clients et de ses prospects sont traitées. Fin décembre 2020, la société comptait dans ses bases de données 25,7 millions de clients pour la fourniture d'électricité, de gaz et de services et environ […] prospects, s'agissant du marché des particuliers.

5. La Commission nationale de l'informatique et des libertés (ci-après " la CNIL " ou " la Commission ") a été saisie de plusieurs plaintes à l'encontre de la société EDF, portant sur l'exercice des droits entre août 2019 et décembre 2020.

6. Un contrôle en ligne a été effectué sur le site web " www.edf.fr " le 15 février 2021. Le procès-verbal n° 2021-020-1, dressé par la délégation à l'issue du contrôle, a été notifié à la société EDF le 17 février 2021.

7. Une mission de contrôle sur pièces a également été réalisée par l'envoi d'un questionnaire à la société le 25 mars 2021, auquel la société a répondu le 29 avril 2021.

8. Deux demandes de compléments d'informations ont été adressées à la société les 13 juillet et 18 août 2021. La société y a répondu les 30 juillet, 31 août et 3 septembre 2021.

9. Aux fins d'instruction de ce dossier, la présidente de la Commission a désigné Madame Valérie PEUGEOT en qualité de rapporteure, le 19 mai 2022, sur le fondement de l'article 39 du décret n° 2019-536 du 29 mai 2019 modifié.

10. Le 23 juin 2022, la rapporteure a fait notifier à la société un rapport détaillant les manquements au RGPD qu'elle estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la Commission de prononcer une amende administrative au regard des manquements constitués aux articles 7, paragraphe 1, 12, 13, 14, 15, 21 et 32 du RGPD et L. 34-5 du code des postes et des communications électroniques (ci-après " le CPCE "). Il proposait également qu'une injonction de mettre en conformité le traitement avec les dispositions des articles 7, paragraphe 1, 14 et 32 du RGPD et L. 34-5 du CPCE, assortie d'une astreinte, soit prononcée. Enfin, il proposait que la décision de sanction soit rendue publique, mais qu'il ne soit plus possible d'identifier nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

11. Le 25 juillet 2022, la société a produit ses observations en réponse au rapport de sanction.

12. La rapporteure a répondu aux observations de la société le 11 août 2022.

13. Le 9 septembre 2022, la société a produit de nouvelles observations en réponse à celles de la rapporteure.

14. Par courrier du 15 septembre 2022, la rapporteure a informé le conseil de la société que l'instruction était close, en application de l'article 40, III, du décret modifié n°2019-536 du 29 mai 2019.

15. Par courrier du même jour, le conseil de la société a été informé que le dossier était inscrit à l'ordre du jour de la formation restreinte du 13 octobre 2022.

16. La société et la rapporteure ont présenté des observations orales lors de la séance de la formation restreinte.

II. Motifs de la décision

A. Sur le manquement à l'obligation de recueillir le consentement des personnes concernées pour la mise en œuvre de prospection commerciale par voie électronique

17. Aux termes de l'article L. 34-5 du CPCE, " est interdite la prospection directe au moyen de système automatisé de communications électroniques […], d'un télécopieur ou de courriers électroniques utilisant les coordonnées d'une personne physique […] qui n'a pas exprimé préalablement son consentement à recevoir des prospections directes par ce moyen. Pour l'application du présent article, on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe. […] ".

18. Aux termes de l'article 4, paragraphe 11, du RGPD, " Aux fins du présent règlement, on entend par […] " consentement " de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ".

19. Aux termes de l'article 7, paragraphe 1, du RGPD, " Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant ".

20. La rapporteure, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant des articles L. 34-5 du CPCE et 7, paragraphe 1, du RGPD, tel qu'éclairé par les dispositions de l'article 4, paragraphe 11, du RGPD, se fonde sur le fait que la société EDF, qui réalise des opérations de prospection commerciale par voie électronique, n'est pas en mesure de disposer et d'apporter la preuve d'un consentement valablement exprimé par

les prospects dont les données proviennent de courtiers en données avant d'être démarchés. En outre, la rapporteure a relevé que, dans le cadre de l'instruction de trois plaintes, il est apparu que la société avait des difficultés à obtenir du courtier en données concerné des éléments de preuve concernant le recueil du consentement : le courtier en données a produit le formulaire type, et non le formulaire rempli individuellement par chaque prospect, n'étant ainsi pas en mesure de transmettre la preuve individuelle du consentement.

21. En défense, la société fait valoir qu'aucune des trois plaintes visées dans le rapport ne concerne des opérations de prospection commerciale par voie électronique et donc que l'article L. 34-5 du CPCE est inapplicable. La société ajoute que les opérations de prospection commerciale par voie électronique sur la base de données collectées auprès de courtiers en données sont très ponctuelles et visent un nombre non significatif de prospects ([…] %). En outre, la société indique qu'elle a toujours strictement encadré ses relations contractuelles avec les courtiers en données auxquels elle fait appel et que des échanges fréquents avaient lieu, même s'ils n'étaient pas nécessairement formalisés sous forme d'audits. Enfin, la société explique […] que les données déjà collectées dans le cadre de campagnes précédentes ont été supprimées. Elle ajoute cependant avoir fait évoluer les contrats conclus avec les courtiers en données et mis en place, dès novembre 2021, des audits formalisés.

22. En premier lieu, la formation restreinte rappelle que, lorsque les données des prospects n'ont pas été collectées directement auprès d'eux par l'organisme qui prospecte, le consentement peut avoir été recueilli au moment de la collecte initiale des données par le primo-collectant, pour le compte de l'organisme qui réalisera les opérations de prospection ultérieures. À défaut, il revient à l'organisme qui prospecte de recueillir un tel consentement avant de procéder à des actes de prospection. Au regard des dispositions de l'article 7, paragraphe 1, du RGPD, le prospecteur doit alors être en mesure de prouver qu'il dispose de ce consentement. En outre, pour que le consentement soit éclairé, les personnes doivent notamment être clairement informées de l'identité du prospecteur pour le compte duquel le consentement est collecté et des finalités pour lesquelles les données seront utilisées. Pour ce faire, une liste exhaustive et mise à jour doit être tenue à la disposition des personnes au moment du recueil de leur consentement, par exemple directement sur le support de collecte ou, si celle-ci est trop longue, via un lien hypertexte renvoyant vers ladite liste et les politiques de confidentialité des prestataires et fournisseurs.

23. La formation restreinte note que les trois plaintes reçues par la CNIL et visées par la rapporteure ne portent pas sur des opérations de prospection commerciale électronique. Elle relève en revanche que […] prospects ont fait l'objet de prospection commerciale par voie électronique de la part de la société EDF entre 2020 et janvier 2021, pour lesquels EDF n'est pas en mesure de communiquer de pièces démontrant l'obtention d'un consentement valablement recueilli auprès des personnes.

24. Au surplus, si la société a fourni à la délégation de contrôle deux exemples de formulaire type de collecte de données des prospects mis à disposition par le courtier en données […], la formation restreinte relève qu'aucune liste de partenaires - incluant EDF- devant être tenue à la disposition des prospects au moment de consentir, n'a été communiquée dans le cadre de la procédure, en dépit des demandes de la rapporteure en ce sens.

25. En deuxième lieu, la formation restreinte relève que, dans le cadre du contrôle sur pièces, la société a indiqué que les courtiers en données sont en charge de la collecte du consentement des personnes concernées et qu'elle leur demande de s'engager contractuellement à respecter le RGPD et les règles applicables en matière de prospection commerciale. La société a reconnu n'exercer aucun contrôle sur les formulaires de recueil utilisés, ni réaliser d'audits sur ses co-contractants, mais a affirmé conduire des échanges informels avec eux.

26. La formation restreinte considère dès lors que les mesures mises en place par la société EDF pour s'assurer auprès de ses partenaires que le consentement a été valablement donné par les prospects avant d'être démarchés étaient insuffisantes.

27. Dans ces conditions, la formation restreinte considère que la société a méconnu ses obligations résultant des articles L. 34-5 du CPCE et 7, paragraphe 1, du RGPD, tel qu'éclairé par les dispositions de l'article 4, paragraphe 11, du RGPD.

28. Elle relève néanmoins que, dans le cadre de la présente procédure, la société a indiqué avoir supprimé les données déjà collectées dans le cadre de campagnes précédentes.

B. Sur le manquement à l'obligation d'information des personnes

29. L'article 13, paragraphe 1, du RGPD dresse la liste des informations devant être communiquées par le responsable de traitement aux personnes concernées lorsque leurs données à caractère personnel sont collectées directement auprès d'elles, parmi lesquelles " les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement ".

30. Le paragraphe 2 de ce même article dispose qu'" en plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée, au moment où les données à caractère personnel sont obtenues, les informations complémentaires suivantes qui sont nécessaires pour garantir un traitement équitable et transparent :

a) la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée […] ".

31. L'article 14 du RGPD dresse quant à lui la liste des informations devant être communiquées par le responsable de traitement aux personnes concernées lorsque leurs données à caractère personnel n'ont pas été collectées auprès d'elles. Le paragraphe 2 de ce même article prévoit qu' " en plus des informations visées au paragraphe 1, le responsable du traitement fournit à la personne concernée les informations suivantes nécessaires pour garantir un traitement équitable et transparent à l'égard de la personne concernée : […]

f) la source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public […] ".

32. Les lignes directrices sur la transparence au sens du règlement (UE) 2016/679, adoptées par le groupe de travail " article 29 " dans leur version révisée le 11 avril 2018, venant éclairer les dispositions de l'article 13, précisent que : " la durée de conservation […] devrait être formulée de manière à ce que la personne concernée puisse évaluer, selon la situation dans laquelle elle se trouve, quelle sera la période de conservation s'agissant de données spécifiques ou en cas de finalités spécifiques. Le responsable du traitement ne peut se contenter de déclarer de façon générale que les données à caractère personnel seront conservées aussi longtemps que la finalité légitime du traitement l'exige. Le cas échéant, différentes périodes de stockage devraient être mentionnées pour les différentes catégories de données à caractère personnel et/ou les différentes finalités de traitement, notamment les périodes à des fins archivistiques. "

33. Elles précisent également que " la levée de l'obligation de fournir à la personne concernée des informations sur la source de ses données à caractère personnel s'applique uniquement lorsqu'une telle fourniture n'est pas possible en raison de l'impossibilité d'attribuer différents éléments des données à caractère personnel concernant une même personne à une source en particulier. En revanche, le simple fait qu'une base de données comprenant les données à caractère personnel de plusieurs personnes concernées ait été compilée par un responsable du traitement utilisant plus d'une source ne suffit pas à lever cette obligation s'il est possible (bien que chronophage ou fastidieux) de déterminer la source dont proviennent les données à caractère personnel des personnes concernées " (paragraphe 60).

34. La rapporteure relève, d'une part, un manquement à l'article 13 du RGPD dans la mesure où, au moment du contrôle en ligne effectué le 15 février 2021, la base légale n'était pas mentionnée et les durées de conservation des données n'étaient pas développées de manière suffisamment précise dans la " charte de protection des données personnelles " figurant sur le sous-domaine " particulier.edf.fr " ; elle relève, d'autre part, un manquement à l'article 14 du RGPD, dans la mesure où les personnes démarchées par voie postale par la société n'étaient pas informées de la source précise de leurs données à caractère personnel, à savoir l'identité de la société auprès de laquelle EDF les a obtenues.

35. En défense, la société considère que la " charte de protection des données personnelles " qui figurait sur le site web " particulier.edf.fr " lors du contrôle en ligne du 15 février 2021 contenait l'ensemble des informations exigées au titre de l'article 13 du RGPD et garantissait un " traitement équitable et transparent " des données concernées. S'agissant des durées de conservation, la société relève que certaines durées de conservation étaient mentionnées, bien que non exhaustives car la société procédait, à la date du contrôle en ligne, à une large refonte des durées de conservation. Elle considère qu'il n'était donc pas possible d'indiquer l'ensemble des durées de conservation, puisque celles-ci étaient en cours de revue et de modification. S'agissant des bases légales, la société indique que l'article 13, paragraphe 1, c) du RGPD n'exige pas du responsable de traitement qu'il indique aux personnes concernées chaque base légale pour chaque finalité poursuivie, mais simplement qu'il informe des bases légales utilisées. Elle précise avoir néanmoins entrepris une modification profonde de la charte évoquée dont la mise à jour a été publiée en avril 2021 sur le site " particulier.edf.fr ".

36. S'agissant du manquement à l'article 14, la société indique que la nature de la source était a minima visée dans les mentions d'information portées à l'attention des personnes concernées, à savoir un " organisme spécialisé dans l'enrichissement de données ". Elle ajoute que le fait de se limiter à une information assez générale sur l'origine des données permettait d'éviter une confusion en laissant entendre à la personne concernée qu'elle n'était inscrite que dans la base de données du courtier en données, alors qu'elle était susceptible de figurer simultanément dans plusieurs bases de données détenues par différents courtiers en données. La société argue enfin de l'absence de préjudice causé aux personnes qui pouvaient contacter EDF afin d'obtenir davantage d'informations.

37. En premier lieu, la formation restreinte relève que la " charte de protection des données personnelles " présente sur le sous-domaine " particulier.edf.fr " constituait l'information délivrée par la société au titre de l'article 13 du RGPD pour d'autres types de traitements que la prospection (par exemple création du compte client ou souscription d'un contrat en ligne). Or, la charte ne précisait pas la base légale correspondant à chaque finalité énumérée, élément pourtant exigé par l'article 13 du RGPD.

38. En outre, si la formation restreinte prend note des explications fournies par la société s'agissant de la refonte des durées de conservation en cours au moment des constatations en ligne effectuées par la délégation de contrôle, il n'en demeure pas moins que, au moment de ces constatations, ladite charte précisait " Nous ne conservons vos données que pendant la durée nécessaire à leur traitement selon la finalité qui a été fixée ", avec un exemple relatif aux durées de conservation pour les clients équipés d'un compteur Linky. La formation restreinte considère que l'information sur les durées de conservation était vague et imprécise, de sorte qu'elle ne suffisait pas à garantir " un traitement équitable et transparent " des données à caractère personnel traitées.

39. Dès lors, la formation restreinte considère que la société a méconnu ses obligations résultant de l'article 13 du RGPD. Elle prend néanmoins acte du fait que la société a remédié à ce manquement, puisque les bases légales et durées de conservation sont dorénavant détaillées dans la charte évoquée ci-avant.

40. En deuxième lieu, s'agissant du manquement à l'article 14 du RGPD, la formation restreinte relève que, sur le premier courrier de prospection adressé aux plaignants (saisines n° […] , n° […] et n° […]), dont les données ont été obtenues indirectement, la mention suivante figure : " EDF, responsable de traitement, met en œuvre un traitement de données personnelles à des fins de prospection […]. Vos données ont été collectées auprès d'un organisme spécialisé dans l'enrichissement de données ".

41. La formation restreinte considère que la seule mention que les données ont été collectées auprès d'un " organisme spécialisé dans l'enrichissement de données ", figurant dans le premier courrier de prospection commerciale adressé par EDF, n'est pas suffisamment précise quant à la source d'où proviennent les données. Cette information n'est ainsi pas de nature à " garantir un traitement équitable et transparent " à l'égard du prospect, en particulier dans un contexte de reventes successives de données entre de multiples acteurs et dans l'hypothèse où le prospect souhaiterait exercer ses droits auprès du courtier en données dont il ignore l'identité.

42. La formation restreinte estime que l'absence d'un préjudice important pour les personnes invoquée par la société et la possibilité de contacter EDF afin d'obtenir davantage d'informations est sans influence sur la caractérisation du

manquement à l'information des personnes, laquelle est une obligation distincte du droit d'obtenir toute information disponible quant à la source des données en application de l'article 15, paragraphe 1, g) du RGPD.

43. Dès lors, la formation restreinte considère que les faits précités constituent un manquement à l'article 14 du RGPD.

44. La formation restreinte relève qu'au cours de la procédure, la société a modifié les mentions d'information figurant dans les courriers de prospection, afin d'y faire apparaître le nom du courtier en données concerné.

C. Sur les manquements en lien avec l'exercice des droits des personnes

45. Aux termes de l'article 12 du RGPD :

" 1. Le responsable du traitement prend des mesures appropriées […] pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples […]. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens. […]

3. Le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulée en application des articles 15 à 22, dans les meilleurs délais et en tout état de cause dans un délai d'un mois à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de deux mois, compte tenu de la complexité et du nombre de demandes. Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande. […]

4. Si le responsable du traitement ne donne pas suite à la demande formulée par la personne concernée, il informe celle-ci sans tarder et au plus tard dans un délai d'un mois à compter de la réception de la demande des motifs de son inaction et de la possibilité d'introduire une réclamation auprès d'une autorité de contrôle et de former un recours juridictionnel. […] ".

46. L'article 15, paragraphe 1, du RGPD prévoit le droit pour une personne d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès aux données à caractère personnel la concernant, notamment " g) lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ". Il est également prévu au paragraphe 3 du même article que " le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement. […] ".

47. L'article 21, paragraphe 2, du RGPD dispose que, " Lorsque les données à caractère personnel sont traitées à des fins de prospection, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection. […] "

1. Sur le manquement à l'obligation de transparence

48. La rapporteure, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 12 du RGPD, se fonde sur deux saisines de la CNIL, émanant de Monsieur […] (saisine n° […]) et de Monsieur […] (saisine n° […]). S'agissant de la première saisine, la rapporteure a relevé que la société EDF avait contacté le plaignant par téléphone pour lui apporter une réponse, sans lui adresser d'écrit, en violation de l'article 12, paragraphe 1, du RGPD. En outre, la réponse qui lui a été apportée sur l'organisme à l'origine des données était erronée. Enfin, la société a répondu à ses questions, de nouveau par téléphone, plus de neuf mois plus tard. S'agissant de la seconde saisine, la rapporteure a relevé que la société avait clôturé la demande du plaignant au lieu de la transmettre au service en charge des demandes d'exercice de droits et n'avait pas répondu à Monsieur […]. Ce n'est que six mois après sa demande initiale – dans le cadre de la procédure de contrôle – qu'une réponse a été apportée au plaignant.

49. En défense, la société indique que la politique de la société EDF a toujours été de répondre par écrit à l'ensemble des demandes d'exercice de droits de ses prospects et clients. Elle précise que, pour toute réclamation écrite, le conseiller tente de contacter le prospect ou le client par téléphone, avant de lui envoyer une réponse documentée sous forme écrite. La société ajoute que l'absence de réponse écrite à Monsieur […] relève d'une simple erreur humaine commise par le conseiller, lequel n'a pas suivi les procédures internes. La société ajoute que le traitement des demandes d'exercice de droit des plaignants s'est inscrit dans le contexte particulièrement difficile à la fois de la crise sanitaire, qui a conduit à un accroissement du nombre de demandes d'exercice de droit, et de report de la fin de la trêve hivernale au 1er septembre 2020, ce qui peut expliquer que leur courrier n'ait pu être correctement traité dans les délais usuels.

50. La formation restreinte note que la société reconnaît une erreur d'orientation des demandes des plaignants ayant entraîné " soit une absence de réponse dans le délai imparti, soit une mauvaise qualité de réponse ". Un manquement aux obligations de l'article 12 du RGPD est constitué dès lors que la société n'a pas apporté de réponse par écrit et a donné au plaignant des informations erronées s'agissant de la saisine de Monsieur […]. En outre, la société n'a pas traité ces demandes d'exercice de droits dans le délai imparti s'agissant des deux saisines.

51. Par conséquent, la formation restreinte considère que le manquement à l'article 12 du RGPD est constitué.

2. Sur le manquement à l'obligation de respecter le droit d'accès

52. La rapporteure, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 15 du RGPD en matière de droit d'accès, se fonde sur deux saisines de la CNIL, émanant de Monsieur (saisine n° […]) et de Madame (saisine n° […]). S'agissant de la saisine de Monsieur […], la première réponse apportée par voie téléphonique au plaignant sur la source des données collectées était erronée. Quant à la saisine de Madame […], la

société précise qu'une réponse lui a été adressée le 17 juillet 2020, lui indiquant qu'elle n'avait aucune autre donnée la concernant que son prénom et son nom dans ses bases de données. La rapporteure a considéré qu'une telle affirmation était inexacte et que la société avait au moins son adresse – ou ancienne adresse – pour effectuer le rapprochement avec les nom et prénom de la plaignante puisque la société EDF lui a adressé un courrier au domicile de ses parents.

53. En défense, s'agissant de la saisine relative à Monsieur […], la société reconnaît que la réponse du conseiller au plaignant était " en partie inexacte " en raison d'une erreur s'agissant de la source des données. Quant à la saisine relative à Madame […], la société considère que la réponse qui lui a été apportée par le conseiller était correcte puisque les seules données rattachables à la plaignante étaient ses nom et prénom.

54. Au vu des éléments apportés par la société, la rapporteure propose à la formation restreinte de ne pas retenir le manquement à l'article 15 du RGPD s'agissant de la saisine relative à Madame […].

55. La formation restreinte relève que les faits relevés par la rapporteure ne sont pas contestés par la société s'agissant de la saisine de Monsieur […] et qu'il est avéré qu'une réponse inexacte lui a été apportée dans le cadre de sa demande de droit d'accès. Elle considère qu'un manquement aux obligations de l'article 15 est constitué s'agissant de cette plainte, dès lors que la société lui a apporté une information erronée sur la source des données collectées dans le cadre de sa demande de droit d'accès. En revanche, s'agissant de la plainte de Madame […], la formation restreinte prend acte des éléments apportés par la société et considère que le manquement invoqué n'est pas caractérisé.

3. Sur le manquement à l'obligation de respecter le droit d'opposition

56. La rapporteure, pour proposer à la formation restreinte de considérer que la société a méconnu ses obligations résultant de l'article 21 du RGPD, se fonde sur la saisine de Monsieur […] (n° […]). La rapporteure indique que la société n'a pas pris en compte l'opposition du plaignant au traitement des données à caractère personnel de son fils mineur à des fins de prospection commerciale. En effet, le fils mineur de Monsieur […] a reçu un second courrier de prospection commerciale, en dépit de la demande de ce dernier visant à la suppression des données à caractère personnel relatives à son fils.

57. En défense, la société explique que, dans le guide " Réclamation " de mai 2020 à destination de l'ensemble des conseillers, ces derniers avaient pour consigne, pour toute demande d'effacement des données d'un prospect, de " systématiquement collecter l'opposition du prospect ". Concernant la saisine de Monsieur […], le conseiller a bien procédé à l'effacement des données comme il l'avait indiqué par téléphone au plaignant mais n'a pas complètement suivi la procédure interne en ne procédant à l'opposition avant d'effacer les données. La société ajoute avoir simplifié cette procédure d'effacement. Ainsi, depuis juillet 2021, lorsque le conseiller traite une demande d'effacement, une mise en opposition est automatiquement mise en œuvre.

58. La formation restreinte relève que les faits relevés par la rapporteure s'agissant de la situation du plaignant ne sont pas contestés par la société et constituent un manquement aux obligations découlant de l'article 21 du RGPD. Elle note qu'au cours de la procédure de sanction, la société a amélioré sa procédure de gestion des demandes d'effacement.

D. Sur le manquement à l'obligation d'assurer la sécurité des données

59. Aux termes de l'article 32, paragraphe 1, du RGPD, " Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

a) […] ;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

c) […] ;

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement. ".

• Sur la fonction de hachage des mots de passe du portail " prime énergie "

60. Compte tenu des déclarations initiales de la société lors de la procédure de contrôle, la rapporteure a relevé que les mots de passe à l'espace client du portail " prime énergie " étaient stockés au moyen de la fonction de hachage MD5. La rapporteure a ensuite pris acte des nouvelles affirmations de la société et du fait que, depuis janvier 2018, la fonction de hachage SHA-256 est utilisée. Elle a néanmoins relevé que, jusqu'à juillet 2022, les mots de passe de plus de 25 800 comptes étaient conservés de manière non sécurisée, avec la fonction de hachage MD5.

61. En défense, la société explique que, depuis janvier 2018, toutes les inscriptions ou les modifications d'un mot de passe utilisateur sont enregistrées dans l'annuaire associé au portail " prime énergie " en SHA-256 avec un mécanisme d'aléas associé (salage). Le hachage MD5 correspond uniquement au niveau de hachage mis en place historiquement par la société […] , sous-traitant d'EDF, et pour lequel seuls quelques milliers de comptes étaient encore concernés en avril 2021. La société ajoute que ces mots de passe étaient tout de même stockés avec la robustesse du mécanisme supplémentaire d'aléa (salage), empêchant les attaques par tables précalculées. Elle en conclut que les mots de passe étaient sécurisés. En outre, la société indique que, depuis le début de l'année 2022, une ultime purge des mots de passe qui étaient encore stockés au moyen de la fonction de hachage MD5 (environ 3,2% du nombre total de clients " prime énergie ") a été réalisée. Elle précise ainsi que tous les mots de passe des utilisateurs du site " prime énergie " sont aujourd'hui stockés avec un sel et un algorithme fort.

62. La formation restreinte rappelle qu'il résulte des dispositions de l'article 32 du RGPD que le responsable de traitement est tenu de s'assurer que le traitement automatisé de données qu'il met en œuvre est suffisamment sécurisé. Le caractère suffisant des mesures de sécurité s'apprécie, d'une part, au regard des caractéristiques du traitement et des risques qu'il induit, d'autre part, en tenant compte de l'état de connaissances et du coût des mesures. La mise en place d'une politique d'authentification robuste constitue une mesure élémentaire de sécurité qui participe généralement au respect des obligations de l'article 32 du RGPD. Ainsi, il est nécessaire de veiller à ce qu'un mot de passe permettant de s'authentifier sur un système ne puisse pas être divulgué. La conservation des mots de passe de manière sécurisée constitue une précaution élémentaire en matière de protection des données à caractère personnel. Dès 2013, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) alertait et rappelait les bonnes pratiques s'agissant de la conservation des mots de passe en indiquant qu'ils doivent " être stockés sous une forme transformée par une fonction cryptographique à sens unique (fonction de hachage) et lente à calculer telle que PBKDF2 " et que " la transformation des mots de passe doit faire intervenir un sel aléatoire pour empêcher une attaque par tables précalculées ". En effet, les fonctions de hachage non robustes présentent des vulnérabilités connues qui ne permettent pas de garantir l'intégrité et la confidentialité des mots de passe en cas d'attaque par force brute après compromission des serveurs qui les hébergent. Dans la mesure où un grand nombre d'internautes utilisent le même mot de passe pour s'authentifier à leurs différents comptes en ligne, des attaquants pourraient exploiter les données compromises pour multiplier les intrusions sur leurs autres comptes pour commettre par exemple des vols ou des escroqueries.

63. De même, la Commission précise également dans sa délibération n° 2017-012 du 19 janvier 2017, s'agissant des modalités de conservation, que " le mot de passe ne doit jamais être stocké en clair. Elle recommande qu'il soit transformé au moyen d'une fonction cryptographique non réversible et sûre (c'est-à-dire utilisant un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), intégrant l'utilisation d'un sel ou d'une clé. La Commission estime de plus que le sel ou la clé doit être généré au moyen d'un générateur de nombres pseudo-aléatoires cryptographiquement sûr (c'est-à-dire basé sur un algorithme public réputé fort dont la mise en œuvre logicielle est exempte de vulnérabilité connue), et ne pas être stocké dans le même espace de stockage que l'élément de vérification du mot de passe ".

64. Outre ces recommandations, la formation restreinte souligne qu'elle a, à plusieurs reprises, adopté des sanctions pécuniaires où la caractérisation d'un manquement à l'article 32 du RGPD est le résultat de mesures insuffisantes pour garantir la sécurité des données traitées. Elle a ainsi eu l'occasion de rappeler que " le recours à la fonction de hachage MD5 par la société n'est plus considérée depuis 2004 comme à l'état de l'art et son utilisation en cryptographie ou en sécurité est proscrite. Ainsi, l'utilisation de cet algorithme permettrait à une personne ayant connaissance du mot de passe haché de déchiffrer celui-ci sans difficulté en un temps très court (par exemple, au moyen de sites internet librement accessibles qui permettent de retrouver la valeur correspondante au hash du mot de passe) " (délibération SAN-2021-008 du 14 juin 2021).

65. Or, la formation restreinte constate que, jusqu'à juillet 2022, les mots de passe de plus de 25 800 comptes étaient conservés de manière non sécurisée, avec la fonction de hachage MD5. Dans ces conditions, eu égard aux risques encourus par les personnes, la formation restreinte considère que la société a manqué aux obligations qui lui incombent en vertu de l'article 32 du RGPD.

66. Elle relève néanmoins que, dans le cadre de la présente procédure, la société a justifié avoir pris des mesures pour se mettre en conformité avec les obligations découlant de l'article 32 du RGPD.

• Sur la fonction de hachage des mots de passe à l'espace client EDF

67. Compte tenu des déclarations initiales de la société lors de la procédure de contrôle, la rapporteure a relevé que les mots de passe à l'espace client EDF, accessible à l'URL " www.particuliers.edf.fr ", étaient stockés sous forme hachée et salée au moyen de la fonction SHA-1, pourtant réputée obsolète. Elle a donc considéré que les modalités de stockage des mots de passe ne permettent pas de garantir la sécurité et la confidentialité des données à caractère personnel des clients.

68. En défense, la société indique que l'algorithme de hachage utilisé pour stocker les mots de passe dans l'annuaire […], qui gère l'authentification des espaces clients, est en réalité SHA-512 complété d'un mécanisme d'ajout d'aléa (salage) depuis le 17 mai 2017, et non SHA-1, contrairement à ce qu'elle avait pu indiquer à la délégation de contrôle. La société ajoute que le renouvellement des mots de passe et la purge des anciens mots de passe ont été réalisés de manière progressive.

69. Dans le dernier état de ses écritures, la rapporteure relève que, si 11 241 166 mots de passe de comptes sont bien hachés et salés, 2 414 254 mots de passe de comptes sont hachés uniquement, sans avoir été salés.

70. En défense, la société rappelle qu'elle déploie des moyens importants tant humains que matériels en matière de cybersécurité. Elle ajoute que, depuis ses dernières observations, la société a mis en œuvre le mécanisme d'ajout d'aléa (salage) sur la fraction des mots de passe de l'annuaire […] qui n'en disposaient pas, mais qui étaient toutefois déjà hachés avec SHA-512. Ainsi, il n'existe plus à ce jour aucun mot de passe haché en SHA-512 sans mécanisme d'ajout d'aléa (salage).

71. La formation restreinte renvoie aux développements ci-dessus s'agissant de la nécessité de faire intervenir un sel aléatoire pour la transformation des mots de passe (§§ 62 et 63). Elle relève en outre que, dans son guide " Recommandations relatives à l'authentification multifacteur et aux mots de passe " du 8 octobre 2021, l'ANSSI écrit : " Il est recommandé d'utiliser un sel choisi aléatoirement pour chaque compte et d'une longueur d'au moins 128 bits ".

72. La formation restreinte relève que, là encore, la société ne conteste pas le manquement en lui-même mais demande à ne pas être sanctionnée dans la mesure où elle a dorénavant remédié au manquement. La formation restreinte considère que la société a manqué aux obligations qui lui incombent en vertu de l'article 32 du RGPD, dès lors qu'elle n'a pas pris les mesures nécessaires pour assurer la sécurité de la totalité des données qu'elle traite et qui sont accessibles à partir des comptes des utilisateurs à l'URL " www.particuliers.edf.fr ", en n'utilisant pas systématiquement un sel dans la transformation des mots de passe.

73. Elle note néanmoins que, dans le cadre de la présente procédure, la société a justifié avoir pris des mesures pour se mettre en conformité avec les obligations découlant de l'article 32 du RGPD.

III. Sur les mesures correctrices et leur publicité

74. Aux termes de l'article 20, III, de la loi du 6 janvier 1978 modifiée, " Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : […]

7° A l'exception des cas où le traitement est mis en œuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83 ".

75. L'article 83 du RGPD prévoit quant à lui que " chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives ", avant de préciser les éléments devant être pris en compte pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de cette amende.

76. En premier lieu, sur le principe du prononcé d'une sanction, la société indique qu'outre le fait qu'elle conteste les manquements reprochés par la rapporteure ou les justifie, elle a d'ores et déjà pris toutes les mesures pour remédier à l'ensemble des faits reprochés et assurer sa conformité à la législation applicable. Elle insiste sur la bonne volonté et les efforts dont elle a fait preuve tout au long de la procédure. La société considère que les facteurs d'atténuation posés par l'article 83, paragraphe 2, du RGPD devraient amener la formation restreinte à ne pas prononcer de sanction financière ou à tout le moins à réduire très significativement le montant de l'amende proposée par la rapporteure. Elle considère que les manquements allégués ne sont pas substantiels en l'espèce, dès lors qu'ils ont représenté un impact limité voire inexistant sur les droits et libertés des personnes concernées compte tenu de leur faible nombre et de leur caractère non structurel.

77. La formation restreinte rappelle qu'elle doit tenir compte, pour le prononcé d'une amende administrative, des critères précisés à l'article 83 du RGPD, tels que la nature, la gravité et la durée de la violation, les mesures prises par le responsable du traitement pour atténuer le dommage subi par les personnes concernées, le degré de coopération avec l'autorité de contrôle et les catégories de données à caractère personnel concernées par la violation.

78. La formation restreinte souligne que les manquements commis par la société portent sur des obligations touchant aux principes fondamentaux de la protection des données à caractère personnel et que de nombreux manquements sont constitués.

79. La formation restreinte relève ensuite que la société est le premier acteur de l'électricité en France, puisqu'elle dénombrait, fin décembre 2020, 25,7 millions de clients pour la fourniture d'électricité, de gaz et de services et environ […] prospects, s'agissant du marché des particuliers. Elle dispose donc de ressources importantes lui permettant de traiter les questions de protection des données à caractère personnel.

80. En conséquence, la formation restreinte considère qu'il y a lieu de prononcer une amende administrative au regard des manquements constitués à l'article L. 34-5 du CPCE et aux articles 7, paragraphe 1, 12, 13, 14, 15, 21 et 32 du RGPD.

81. La formation restreinte souligne néanmoins les efforts dont la société EDF a fait preuve dans le cadre de la procédure, puisqu'elle s'est mise en conformité s'agissant de l'ensemble des manquements relevés par la rapporteure. Elle considère par ailleurs que le manquement à l'obligation de recueillir le consentement des personnes concernées pour la mise en œuvre de prospection commerciale par voie électronique, bien qu'étant un manquement structurel, est en l'espèce d'une gravité limitée dans la mesure où le nombre de prospects dont les données ont été collectées auprès de courtiers en données et ayant reçu de la prospection commerciale par voie électronique ne représente que […] % sur la période 2020-2022 de l'ensemble des personnes ciblées par des actions de prospection commerciale réalisées par EDF auprès de prospects dont les données ont été obtenues via des courtiers en données. S'agissant du manquement à l'obligation d'information, la formation restreinte prend acte des déclarations de la société, selon lesquelles elle procédait à une large refonte des durées de conservation, l'empêchant ainsi de toutes les indiquer puisqu'elles étaient en cours de revue et de modification. Elle note en outre, au regard des saisines versées aux débats, que les manquements aux droits des personnes ne sont pas structurels et résultent d'erreurs humaines.

82. La formation restreinte rappelle que les violations du RGPD relevées en l'espèce sont des manquements à des principes susceptibles de faire l'objet, en vertu de l'article 83 du RGPD, d'une amende administrative pouvant s'élever jusqu'à 20 000 000 euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent, le montant le plus élevé étant retenu.

83. La formation restreinte rappelle également que les amendes administratives doivent être à la fois dissuasives et proportionnées. Elle considère en particulier que l'activité de la société et sa situation financière doivent notamment être prises en compte pour la détermination du montant de l'amende administrative. Elle relève à cet égard que le groupe EDF a réalisé un chiffre d'affaires de plus de 69 milliards d'euros pour un résultat net de […] euros en 2020 et de plus de 84 milliards d'euros pour un résultat net de […] euros en 2021.

84. Dès lors, au vu de ces éléments, la formation restreinte considère que le prononcé d'une amende administrative d'un montant de 600 000 euros apparaît justifié.

85. En deuxième lieu, une injonction de mettre en conformité le traitement avec les dispositions des articles 7, paragraphe 1, 14 et 32 du RGPD et L. 34-5 du CPCE a été initialement proposée par la rapporteure.

86. La société soutient que les actions qu'elle a mises en œuvre s'agissant de l'ensemble des manquements relevés doivent conduire à ne pas prononcer d'injonction sous astreinte.

87. Comme indiqué précédemment, la formation restreinte relève que la société a pris des mesures de mise en conformité s'agissant de l'ensemble des manquements relevés par la rapporteure. Elle considère dès lors qu'il n'y a pas lieu de prononcer d'injonction.

88. En troisième lieu, s'agissant de la publicité de la décision de sanction, la société demande à la formation restreinte de ne pas la publier ou, à titre subsidiaire, de l'anonymiser immédiatement ou au plus tard dans un délai de huit jours.

89. La formation restreinte considère que la publicité de la sanction se justifie au regard de la nature et du nombre de manquements commis, ainsi que du nombre de personnes concernées par lesdites violations, en particulier plus de 2 400 000 clients s'agissant du manquement à la sécurité des données.

PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide de :

• prononcer à l'encontre de la société ÉLECTRICITÉ DE FRANCE une amende administrative d'un montant de 600 000 (six cent mille) euros pour les manquements à l'article L. 34-5 du CPCE et aux articles 7, paragraphe 1, 12, 13, 14, 15, 21 et 32 du RGPD ;

• rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément la société à l'expiration d'un délai de deux ans à compter de sa publication.

Le président

Alexandre LINDEN

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.