Comité de sécurité de l'information[1]
Chambre sécurité sociale et santé
Chambre autorité fédérale

DÉLIBÉRATION N° 23/011 DU 5 SEPTEMBRE 2023 RELATIVE À LA COMMUNICATION DE DONNÉES À CARACTÈRE PERSONNEL PAR L'OFFICE NATIONAL DE SÉCURITÉ SOCIALE ET LE SERVICE PUBLIC FÉDÉRAL MOBILITÉ ET TRANSPORT À LA COUR DES COMPTES EN VUE D'EXÉCUTER UN AUDIT PORTANT SUR LA PERCEPTION DE LA COTISATION DE SOLIDARITÉ CO2

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, en particulier l'article 15, § 1er, alinéa 1er ;

Vu la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*, en particulier l'article 35/1, §1 ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier l'article 114 ;

Vu la loi du 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du 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 et à la libre circulation de ces données, et abrogeant la directive 95/46/CE*, en particulier l'article 97 et l'article 98 ;

Vu la demande de la Cour des comptes ;

Vu les renseignements complémentaires de la Cour des comptes ;

Vu le rapport de la Banque Carrefour de la sécurité sociale ;

Vu le rapport du Service public fédéral Stratégie et Appui ;

[1] La présente délibération vaut comme une délibération de la chambre sécurité sociale et la santé et comme une délibération de la chambre autorité fédérale dans la mesure où elle porte sur des traitements de données à caractère personnel qui doivent effectivement être examinés par chacune des chambres à la réglementation en vigueur. La communication de données par l'Office national de sécurité sociale relève de la compétence exclusive de la chambre sécurité sociale et santé (application d' l'article 15, §1, alinéa 1er de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale). La communication de données à caractère personnel de la banque de données MOBIVIS de la Direction Immatriculation des véhicules (DIV) du Service public fédéral Mobilité et Transport relève de la compétence exclusive de la chambre autorité fédérale (application de l'article 35/1 de la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*).

Vu le rapport du président de la chambre sécurité sociale et du président de la chambre autorité fédérale.

I. OBJET DE LA DEMANDE

1. En exécution de ses missions légales, la Cour des comptes souhaite réaliser un audit sur la perception de la cotisation de solidarité CO2 et de la cotisation du 3e pilier du budget mobilité. La demande de données visée par cette délibération ne concerne que la cotisation CO2.

2. Conformément à l'article 38, §3quater de la loi du 29 juin 1981 *établissant les principes généraux de la sécurité sociale des travailleurs salariés*, une cotisation de solidarité est due par l'employeur qui met à la disposition de son travailleur, de manière directe ou indirecte, un véhicule également destiné à un usage autre que strictement professionnel et ce, indépendamment de toute contribution financière du travailleur dans le financement ou l'utilisation de ce véhicule. Le montant de cette cotisation est fonction du taux d'émission de CO2 du véhicule. Cette cotisation est payée par l'employeur à l'Office national de Sécurité sociale, dans les mêmes délais et dans les mêmes conditions que les cotisations de sécurité sociale pour les travailleurs salariés.

3. Concrètement, l'équipe d'audit de la Cour des comptes souhaite procéder au calcul de la cotisation CO2 pour le quatrième trimestre de 2022 due sur la base des données à la fois de l'Office national de sécurité sociale (ONSS) et de la banque de données MOBIVIS de la Direction Immatriculation des véhicules (DIV) du Service public fédéral Mobilité et Transport, en utilisant les plaques d'immatriculation comme clé d'identification entre les deux sets de données. L'équipe comparera ensuite ces montants avec ceux déclarés et demandera à l'ONSS d'expliquer les différences importantes, s'il y en a.

4. Conformément à l'article 5 bis de la loi *organique de la Cour des comptes* du 29 octobre 1846, la Cour des comptes peut se faire communiquer à tout moment tous documents et renseignements, de quelque nature que ce soit, relatifs à la gestion et au processus budgétaire et comptable des services de l'Etat et des organismes publics soumis à son contrôle ou qu'elle juge utiles à l'accomplissement de ses missions.

5. Dans un premier temps, une demande à l'ONSS par employeur (numéro BCE) sera effectuée pour le quatrième trimestre de 2022 des données suivantes collectées dans le cadre de l'article 38, §3, quater, de la loi du 29 juin 1981 *établissant les principes généraux de la sécurité sociale des travailleurs salariés* :

- le numéro d'entreprise ;
- le montant de la cotisation CO2 ;
- la liste des plaques d'immatriculation par entreprise ;
- la mention véhicule écologique.

6. Sur la base de cette liste, la Cour des compte aura besoin des données suivantes de la DIV pour le quatrième trimestre 2022 :

- l'identification du véhicule (plaque d'immatriculation) ;
- l'immatriculation du véhicule (date de première immatriculation, date de changement de statut, statut de l'immatriculation) ;
- les caractéristiques techniques, en tant que paramètres du calcul de la cotisation en vertu de l'article 38, §3 quater, de la loi du 29 juin 1981 *établissant les principes généraux de la sécurité sociale des travailleurs salariés* :
    - la motorisation du véhicule, les véhicules électriques ayant un montant forfaitaire de cotisation, tandis que les thermiques ont des formules spécifiques par type de carburant ;
    - le type de carburant, afin de choisir la formule ad hoc de calcul de la cotisation ;
    - le taux d'émission de CO2 (quatre types de taux sont possibles et donc demandés) ;
    - le type de véhicule (la législation ne vise que les véhicules M1 et N1, qui concernent globalement le transport de personnes).

7. Les personnes dont les données à caractère personnel seront traitées sont uniquement les travailleurs salariés bénéficiant d'un véhicule que l'employeur met à leur disposition pour un usage autre que strictement professionnel (véhicule de société). L'ensemble des plaques au quatrième trimestre est nécessaire pour la réalisation de l'objectif de traitement de la Cour des comptes.

II. EXAMEN DE LA DEMANDE

A. COMPETENCE DU COMITE DE SECURITE DE L'INFORMATION

8. La communication par l'ONSS à la Cour des comptes est un échange de données à caractère personnel qui, en vertu de l'article 15, § 1er, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, doit faire l'objet d'une délibération de la chambre sécurité sociale et santé du Comité de sécurité de l'information.

9. La communication par le SPF Mobilité à la Cour des comptes est un échange de données à caractère personnel qui, en vertu de l'article 35/1, §1, de la loi du 15 août 2012 *relative à la création et à l'organisation d'un intégrateur de services fédéral*, doit faire l'objet une délibération préalable de la chambre autorité fédérale du comité de sécurité de l'information, dans la mesure où les responsables du traitement ne parviennent pas, en exécution de l'article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, à un accord concernant la communication ou au moins un de ces responsables du traitement demande une délibération et en a informé les autres responsables du traitement. Dans les cas mentionnés, la demande est introduite d'office conjointement par les responsables du traitement concernés.

10. La chambre autorité fédérale note qu'aucun protocole n'a été conclu et que l'une des parties concernées, l'ONSS, a introduit une demande d'autorisation. Le SPF Mobilité a informé l'auditorat par courrier électronique qu'il ne s'oppose pas à la communication de données envisagée.

B. QUANT AU FOND

B.1. RESPONSABILITE

11. Conformément à l'article 5.2 du 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 et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (règlement général sur la protection des données, ci-après 'RGDP'), l'ONSS et le SPF Mobilité (les instances qui communiquent des données) et la Cour des comptes (les instance qui reçoit les données) – en tant que responsables du traitement – sont responsables du respect des principes énoncés à l'article 5, paragraphe 1, du RGPD et doivent être en mesure de le démontrer[2].

12. Le RGPD impose toute des obligations spécifiques qui incombent aux responsables de traitement. A cet égard, le présent rapport passe en revue les principales obligations qui sont prévues explicitement par le RGPD mais rappelle et insiste à ce stade-ci de son analyse sur celle qui impose à tout responsable du traitement de tenir un registre des activités de traitement conformément et dans le respect des modalités prévues à l'article 30 du RGPD.

B.2. LICEITE

13. Conformément à l'article 5.1 a), du RGPD, les données à caractère personnel doivent être traitées de manière licite. Cela signifie que le traitement envisagé doit être fondé sur l'une des bases de licéité énoncées à l'article 6 du RGPD.

---

[2] Les données à caractère personnel doivent être:

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);
b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);
c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);
d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);
e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);
f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité).

14. Le traitement précité est licite en ce qu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi la Cour des comptes comme responsable du traitement, conformément à l'article 6, 1), e), du RGPD. Cette mission de la Cour des comptes apparaissent à l'article 180 de la Constitution, l'article 5 bis de la loi *organique de la Cour des comptes* du 29 octobre 1846 et l'article 38, §3, quater, de la loi du 29 juin 1981 *établissant les principes généraux de la sécurité sociale des travailleurs salariés*.

B.3. LIMITATION DE FINALITES

15. L'article 5.1 b) du RGPD n'autorise le traitement des données à caractère personnel qu'à des fins spécifiques, explicites et légitimes (principe de limitation des finalités).

16. La communication poursuit une finalité spécifique, explicite et légitime, c'est-à-dire permettre à la Cour des comptes l'exécution d'un audit portant sur la perception de la cotisation de solidarité CO2.

B.4. PROPORTIONALITE

B.4.1. MINIMISATION DES DONNEES

17. L'article 5.1 c) du RGPD dispose que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

18. Le croisement de données de l'ONSS (montant de cotisation et véhicules déclarés par employeur dans les DMFA) et de celles du SPF Mobilité (caractéristiques techniques des véhicules déclarés en DMFA) est nécessaire au contrôle de l'exactitude des montants de cotisation déclarés. Sans ces données constituant des paramètres du calcul de la cotisation CO2, il n'est pas possible de contrôler la bonne perception de cette cotisation par l'ONSS.

19. La liste des plaques d'immatriculation par entreprise permet de relier les plaques d'immatriculation à une entreprise et in fine à un montant de cotisation CO2. En effet, les montants sont déclarés globalement par employeur. Ces numéros de plaques servent à faire le lien avec les données de la DIV. Sans ces données le croisement avec la base de données de la DIV n'est pas possible. Sans les plaques d'immatriculation par entreprise, il n'est pas possible de calculer la cotisation de solidarité par véhicule et de les additionner pour avoir le montant déclaré dans la DMFA. La cotisation étant déclarée de manière globale par employeur, il est nécessaire de procéder à cette addition.

20. Le montant déclaré de la cotisation CO2 est la donnée à contrôler, via la comparaison entre la cotisation due et ce montant déclaré. Sans ces données aucun contrôle n'est possible.

21. Un véhicule ne peut être qualifié d'écologique que sous certaines conditions (norme CO2 et puissance du moteur). Un véhicule écologique est un véhicule utilisé dans le cadre du budget mobilité. La cotisation CO2 sera déclarée au niveau travailleur et non au niveau employeur. La mention véhicule écologique permet de savoir où est déclarée la cotisation CO2 relative à ce véhicule dans la DMFA. Sans cette mention, il n'est pas possible d'identifier le cas

particulier des cotisations CO2 déclarées au niveau du travailleur dans la DMFA (uniquement dans le cadre du budget mobilité).

22. La plaque d'immatriculation est la clef unique permettant de lier les deux bases de données. Sans ces données le croisement avec la base de données de la DIV n'est pas possible.

23. La cotisation est calculée de manière mensuelle et déclarée de manière trimestrielle. Une immatriculation ou un changement de statut durant le quatrième trimestre signifie que la cotisation CO2 n'est pas redevable pour trois mois complets. Le statut d'immatriculation permet en outre d'éliminer les véhicules radiés avant le trimestre analysé, ou immatriculés après. Sans cette donnée, il n'est pas possible d'identifier le nombre de mois de cotisations.

24. La catégorie de véhicule est une classification européenne des véhicules selon le classement suivant : transport de personnes, transport de marchandises, remorques, véhicules à deux ou trois roues et quadricycles, véhicules agricoles et forestiers. Chaque catégorie est identifiée par un code de catégorie et une description de cette catégorie. En vertu de la législation, les véhicules de société concernés par la cotisation sont de catégories M1 ou N1 (transport de personnes), une autre catégorie serait une anomalie.

25. Le type de motorisation, la cotisation relative à un véhicule électrique se calcule différemment que celle pour un véhicule thermique. Pour les véhicules partiellement électriques, différents champs sont concernés (type d'hybride électrique, moteur électrique). Sans cette donnée, il n'est pas possible de choisir la bonne cotisation due.

26. Le type de carburant est le carburant utilisé par le véhicule thermique. La cotisation CO2 est calculée de manière différente suivant le type de carburant. Sans cette donnée, il n'est pas possible de choisir la bonne formule applicable.

27. Le taux d'émission de CO2 est nécessaire pour réaliser le calcul. Différentes valeurs sont possibles pour ce taux, l'ensemble des champs y relatifs est donc demandé (NEDC, WLTP, valeur pondérée ou non).

28. Le Comité de sécurité de l'information considère donc que les données à caractère personnel décrites sont adéquates, pertinentes et limitées à ce qui est nécessaire aux fins pour lesquelles elles sont traitées.

B.4.2. LIMITATION DE CONSERVATION

29. En ce qui concerne la durée de conservation, le Comité rappelle que les données à caractère personnel ne devraient plus être stockées sous une forme permettant d'identifier les personnes concernées que ce qui est nécessaire aux fins pour lesquelles les données à caractère personnel sont traitées. La durée d'utilisation des données sera exclusivement le temps des travaux d'audit, soit en principe inférieure à un an après réception de celles-ci. Les données à caractère personnel seront conservées par la Cour des comptes pendant une durée de six mois après la publication du rapport.

B.5. INTEGRITE ET CONFIDENTIALITE

30. Conformément à l'article 5.1 f) RGDP les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

31. Conformément à l'article 24 RGDP, compte tenu 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 met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au règlement. Conformément à l'article 32 RGDP, 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.

32. Les parties sont tenues à respecter la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale* et à toute autre règle de protection de la vie privée, en particulier 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 et à la libre circulation de ces données et abrogeant la directive 95/46/CE et la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

33. Le Comité de sécurité de l'information fait référence aux directives en matière de protection applicables à toutes les institutions publiques fédérales qui sont reprises dans la Politique fédérale sur la sécurité de l'information (*Federal Information Security Policy*).

34. Le Comité de sécurité de l'information prend acte du fait que l'ONSS est tenue de respecter les normes minimales de sécurité fixées par le Comité général de coordination de la Banque carrefour de la sécurité sociale.

35. Le Comité de sécurité de l'information prend note du fait que le SPF Mobilité et Transport, l'ONSS et la Cour des comptes disposent chacun d'un délégué à la protection des données.

36. Le Comité de sécurité de l'information prend note du fait que la Cour des comptes déclare que :
- elle a évalué les risques et les besoins de protection qui sont inhérents à son organisation et qui concernent le traitement de données à caractère personnel. Le comité a reçu l'analyse et l'avis positif du DPO de la Cour des comptes.

- elle dispose d'une version écrite de sa politique de sécurité et sa politique de protection des données à caractère personnel y est-elle intégrée. Le comité a reçu une copie de la politique de sécurité.
- elle a identifié les divers supports de son organisation contenant des données à caractère personnel ;
- le personnel interne et externe concerné par le traitement de données à caractère personnel est informé des obligations de confidentialité et de protection en lien avec ces données, découlant à la fois des différentes dispositions légales et du plan de sécurité ;
- elle a pris des mesures de gestion pour empêcher tout accès physique inutile ou non autorisé aux supports contenant les données à caractère personnel ;
- elle a pris des mesures pour éviter tout dommage physique qui pourrait compromettre les données à caractère personnel ;
- elle a pris des mesures de gestion pour protéger les différents réseaux auxquels sont connectés les appareils qui traitent les données à caractère personnel ;
- elle dispose d'une liste actuelle des différentes personnes compétentes qui ont accès aux données à caractère personnel et de leur niveau d'accès respectif (création, consultation, modification, destruction) ;
- elle a installé un mécanisme d'autorisation d'accès sur ses systèmes d'information de sorte que les données à caractère personnel traitées et les traitements qui y ont trait, soient uniquement accessibles aux personnes et applications qui y sont expressément autorisées ;
- son système d'information est conçu de telle sorte qu'il enregistre en permanence l'identité des personnes qui accèdent aux données à caractère personnel ;
- elle a prévu de contrôler la validité et l'efficacité des mesures organisationnelles et techniques à travers le temps afin de garantir la protection des données à caractère personnel ;
- elle a prévu des procédures d'urgence et de rapportage en cas d'incidents de sécurité impliquant des données à caractère personnel ;
- elle dispose d'une documentation mise à jour concernant les différentes mesures de gestion mises en place en vue de la protection des données à caractère personnel et des différents traitements qui y ont trait.

37. Le Comité prend note que la Cour des comptes utilise les services de sécurité suivants dans le cadre de cette communication de données à caractère personnel : une boite électronique aux lettres électronique, un horodatage électronique, une gestion des loggings, une gestion intégrée des utilisateurs et des accès et un système de chiffrement de bout-au-bout.

Par ces motifs,

la chambre sécurité sociale et santé et la chambre autorité fédérale du comité de sécurité de l'information, chacune dans sa compétence,

concluent que la communication de données à caractère personnel par l'ONSS et le SPF Mobilité à la Cour des comptes en vue d'exécuter un audit portant sur la perception de la cotisation de solidarité CO2, telle que décrite dans la présente délibération, est autorisée moyennant le respect des mesures relatives à la protection des données qui y ont été définies, en particulier les mesures de limitation de la finalité, de minimisation des données, de limitation de la conservation et de sécurité de l'information.

Bart VIAENE
chambre Sécurité sociale et santé

Daniel HACHE
chambre Autorité fédérale

Le siège de la chambre sécurité sociale et santé du comité de sécurité de l'information est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: Quai de Willebroeck 38 - 1000 Bruxelles (tél. 32-2-741 83 11). Le siège de la chambre Autorité fédérale du Comité de sécurité de l'information est établi dans les bureaux du SPF BOSA, à l'adresse suivante : Avenue Simon Bolivar 30 – 1000 Bruxelles (tél. 32-2-740 80 64).