



Comité sectoriel pour l'Autorité Fédérale

Délibération AF n° 07/2016 du 17 mars 2016

Objet : demande formulée par l'Office national de sécurité sociale afin de réclamer des données à caractère personnel par voie électronique auprès du SPF Finances en vue d'un projet test pour le développement d'une méthode de data matching et de data mining (AF-MA-201-105)

Le Comité sectoriel pour l'Autorité Fédérale (ci-après "le Comité") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier les articles 31*bis* et 36*bis* ;

Vu l'arrêté royal du 17 décembre 2003 *fixant les modalités relatives à la composition et au fonctionnement de certains comités sectoriels institués au sein de la Commission de la protection de la vie privée* ;

Vu la demande de l'Administrateur général de l'Office national de sécurité sociale, reçue le 26/11/2015 ;

Vu les informations complémentaires reçues de l'Office national de Sécurité sociale, le 09/02/2016 et le 03/03/2016 ;

Vu la demande d'avis technique et juridique adressée au Service public fédéral Fedict en date du 01/03/2016 ;

Vu le rapport de Monsieur Livyns ;

Émet, après délibération, la décision suivante, le 17/03/2016 :

I. CONTEXTE ET OBJET DE LA DEMANDE

1. Le 26 novembre 2015, l'Office national de sécurité sociale (ci-après "le demandeur") a introduit une demande d'autorisation visant à obtenir des données relatives à des types de revenus spécifiques reprises dans les fiches 281.10, 281.20 et 281.50¹, conservées notamment dans la banque de données BELCOTAX² du SPF Finances. Le demandeur entendait utiliser les données afin de mieux comprendre, dans le cadre d'enquêtes ponctuelles et systématiques, tant les mécanismes d'abus que les abus individuels concernant les risques de recouvrement et la fraude sociale. Il souhaitait dès lors procéder à une comparaison à grande échelle et au niveau individuel des données demandées avec d'autres banques de données telles que DIMONA, DMFA et LIMOSA. La demande concernait à la fois la livraison, sur une base périodique, de données en vrac, que le demandeur pourrait soumettre au data mining, et la livraison de données sur une base ponctuelle, que le demandeur pourrait soumettre au data matching.
2. Le 17 décembre 2015, le secrétariat du Comité a invité le demandeur à compléter son dossier sur plusieurs points. Le plus important concernait l'absence de base légale spécifique sur laquelle le data mining/data matching pouvait se fonder, alors que dans la jurisprudence constante du Comité³ et de la Commission de la protection de la vie privée⁴, une telle base est considérée comme étant une garantie nécessaire. Cet aspect a aussi fait l'objet d'une discussion approfondie lors d'une réunion de concertation entre le rapporteur et le demandeur le 5 février 2016.
3. Dans son courrier du 9 février 2016, le demandeur indiquait qu'il prendrait l'initiative de préparer la base légale susmentionnée. Entre-temps, il soumet au Comité la nouvelle demande suivante : *"En attendant cette base légale, l'Office national de sécurité sociale souhaite demander au Comité sectoriel pour l'Autorité Fédérale si, sur la base d'un ensemble test de données valable, tel que repris dans la demande d'autorisation, il pourrait déjà démarrer le développement de la méthode de data matching et de data mining afin de comparer ces données et de les étudier."* [Traduction libre réalisée par le Secrétariat de la Commission vie privée en l'absence de traduction officielle]
4. Dans sa lettre du 29 février 2016 et dans son e-mail du 3 mars 2016, le demandeur a donné davantage d'explications sur le contenu et la portée du projet test précité :

¹ Fiche 281.30 - Rémunérations ;

Fiche 281.45 – Rémunérations des dirigeants d'entreprise ;

Fiche 281.50 – Commissions, courtages, ristournes, vacations, honoraires et autres avantages de toute nature.

² Depuis le 1^{er} janvier 2009, en application de l'arrêté royal du 3 juin 2007 (Moniteur belge du 14/06/2007), l'utilisation de Belcotax on web est devenue obligatoire pour tous les employeurs et autres débiteurs de revenus pour tous les types de fiches 281.10 à 281.30 incluse et les fiches 281.50.

³ Délibérations AF n° 08/2015 et n° 11/2015.

⁴ Avis n° 01/2007, 16/2007, 11/2012, 26/2016 et Recommandation n° 02/2012.

"Toutes les données telles que mentionnées dans la demande initiale seront utilisées dans la phase test. Il s'agit concrètement des données demandées provenant des fiches 281.10, 281.20 et 281.50. L'objectif de la phase test est de développer le code (concevoir le modèle) afin qu'une fois l'autorisation de data mining approuvée, nous puissions immédiatement appliquer le modèle à des données réelles. Étant donné que le modèle doit tenir compte de tous les divers critères et variables (tels que les composantes salariales, les indemnités, la signalétique de l'entreprise/des personnes, ...), sa conception nécessite que nous disposions de toutes ces variables. Pour une explication détaillée des données à recevoir du SPF Finances, l'ONSS fera appel à l'expertise de ce SPF (explication de la forme et du contenu des ensembles de données). L'ONSS établira un ensemble test de numéros de Registre national et de numéros BCE pour lesquels il sera demandé au SPF Finances de fournir les données des fiches 281.10, 281.20 et 281.50. Les données demandées concernent les années 2013-2014.

(...)

Les données seront croisées avec les banques de données Dimona, DMFA, Limosa et éventuellement enrichies à l'aide de données BCE. Ces décisions sont prises par le centre de connaissance de l'ONSS, présidé par monsieur l'Administrateur général. Si un croisement est envisagé avec d'autres banques de données, cela sera préalablement soumis au centre de connaissance. Celui-ci vérifiera toujours si l'ONSS est dûment habilité. Si nécessaire, une procédure de demande d'autorisation sera engagée.

Pour le développement du code, la conception du modèle et la validation des résultats, il est important de travailler avec des données non codées. L'utilisation de données codées/masquées/cryptées empêcherait les analystes et les inspecteurs de vérifier l'exactitude des résultats du modèle. Cette vérification est nécessaire afin de valider le modèle, même si cela ne donnera lieu à aucune enquête d'inspection. Par exemple : si le modèle considère une entreprise comme "à risques" parce que selon les calculs, elle comporte un grand nombre de membres du personnel dont on sait qu'ils perçoivent une indemnité d'un tiers payant en plus de leurs revenus en tant que travailleur salarié, il est nécessaire pour les employeurs, les tiers payants et les travailleurs concernés de comparer les données telles qu'elles sont connues auprès de l'ONSS avec les données reçues du SPF Finances. Si les données reçues du SPF Finances étaient codées, nous ne saurions pas avec quel employeur, tiers payant ou travailleur salarié nous devrions les comparer. Par exemple : il est impossible de calculer une différence si une des deux variables est codée.

Le risque est strictement limité car seul un groupe très restreint (une dizaine de personnes) aura accès aux données (développement et validation, IT et business). (...) L'écriture du code

est assurée par des data scientists du sous-traitant (...), en collaboration avec et sous la direction, le contrôle et la responsabilité d'analystes business (inspecteurs) de l'ONSS. Cela s'effectue sous la direction d'un conseiller de la Direction de la Gestion des risques de la Direction générale des Services de l'inspection de l'ONSS.

L'écriture du code et le développement du modèle prendront approximativement six mois. Si par manque de temps ou en raison de circonstances imprévues, le modèle n'est pas encore prêt dans les 6 mois, l'ONSS en informera le Comité et sollicitera éventuellement une prolongation.

Une fois le modèle achevé, les données test seront détruites et l'ONSS en avertira le Comité.

*Les données test ne seront jamais utilisées pour lancer des enquêtes concrètes sur le terrain."
[Traduction libre réalisée par le Secrétariat de la Commission vie privée en l'absence de traduction officielle]*

5. La présente délibération porte donc uniquement sur les points 3 et 4 du projet test décrit par le demandeur.

II. RECEVABILITÉ DE LA DEMANDE

6. En vertu de l'article 36bis de la LVP, "toute communication électronique de données personnelles par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, exige une autorisation de principe (du comité sectoriel compétent)".
7. Le demandeur souhaite un accès électronique aux données à caractère personnel enregistrées au sein du SPF Finances. Le Comité est dès lors compétent.

III. BIEN-FONDÉ DE LA DEMANDE

1. PRINCIPE DE FINALITÉ

8. L'article 4, § 1, 2° de la LVP exige de tout responsable du traitement qu'il ne collecte des données à caractère personnel que pour des finalités déterminées et explicites.
9. En l'occurrence, le demandeur souhaite réclamer les données au SPF Finances en vue de la réalisation du projet test décrit aux points 3 et 4 pour le développement d'une méthode de data matching et de data mining dans le cadre de ses missions légales (à savoir la perception correcte

et à temps des cotisations de sécurité sociale et le contrôle du respect des dispositions réglementaires afférentes à ces cotisations obligatoires). Les données ne seront donc pas utilisées dans le cadre de dossiers concrets d'enquête, mais purement à des fins de test.

10. Le Comité constate donc que les traitements de données envisagés viseront des finalités déterminées et explicites et rappelle que les données demandées ne peuvent être traitées qu'en vue de ces finalités. Les traitements prévus sont également légitimes, compte tenu de l'article 5, e) de la LVP.
11. En outre, le principe de finalité, repris à l'article 4, § 1, 2° de la LVP, prescrit que tout responsable du traitement ne peut traiter des données à caractère personnel que d'une manière qui n'est pas incompatible avec la finalité pour laquelle les données ont été collectées, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables. Les traitements de données en question constituent un traitement ultérieur de données collectées initialement par le SPF Finances et il convient donc de vérifier dans quelle mesure le projet test envisagé par le demandeur n'est pas incompatible avec les finalités initiales du SPF Finances.
12. Le Comité constate que l'article 337, 2° alinéa du Code des impôts sur les revenus dispose ce qui suit : "Les fonctionnaires de l'administration des contributions directes et de l'administration du cadastre restent dans l'exercice de leurs fonctions lorsqu'ils communiquent *aux autres services administratifs de l'État, y compris les parquets et les greffes des cours et de toutes les juridictions, (aux Communautés, aux Régions) et aux établissements ou organismes publics visés à l'article 329, les renseignements nécessaires à ces services, établissements ou organismes pour assurer l'exécution des dispositions légales ou réglementaires dont ils sont chargés*".
13. Les tâches du demandeur liées à la présente demande sont reprises aux articles 14 et 21 à 31 inclus de la loi du 27 juin 1969 *révisant l'arrêté-loi du 28 décembre 1944 concernant la sécurité sociale des travailleurs*. Les compétences des inspecteurs sociaux du demandeur sont légalement ancrées dans le Code pénal social du 6 juin 2010 (articles 18 à 20 et articles 23 à 56).
14. Il ressort de la réglementation susmentionnée que le demandeur est chargé de la perception correcte et à temps des cotisations de sécurité sociale et du contrôle du respect des dispositions réglementaires afférentes à ces cotisations obligatoires. Dans ce contexte, le demandeur assure donc également la détection des risques de recouvrement et des cas de fraude.

15. Vu ce qui précède, le Comité estime que le traitement ultérieur par le demandeur n'est pas incompatible avec le traitement de données du SPF Finances.

2. PRINCIPE DE PROPORTIONNALITÉ

2.1. Nature des données

16. Les traitements de données à caractère personnel qui sont nécessaires à tout organisme public pour pouvoir exercer sa mission de service public doivent, en application de l'article 4, § 1, 3° et 4° de la LVP, concerner des données qui sont d'une part adéquates, pertinentes et non excessives, au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement et d'autre part qui sont exactes et, si nécessaire, mises à jour.

17. Le demandeur établira un ensemble test de numéros de Registre national et de numéros BCE pour lesquels il sera demandé au SPF Finances de fournir les données provenant des fiches 281.10, 281.20 et 281.50. Il s'agit des catégories de données suivantes :

- a) **Les données figurant sur la fiche 281.10 – Rémunérations** Il s'agit concrètement des données suivantes :
1. Année ;
 2. N° de la fiche ;
 3. Date d'entrée en service et date de départ ;
 4. Nom et adresse du débiteur des revenus ;
 5. Numéro national du bénéficiaire des revenus s'il est domicilié en Belgique⁵ ;
 6. Les revenus imposables payés ou attribués à des résidents ;
 7. Rémunérations
 - a. Rémunérations ;
 - b. Avantages de toute nature (+ spécifications éventuelles) ;
 - c. Timbres de fidélité ;
 - d. Total des rémunérations ;
 - e. Autres rémunérations ;
 8. Options sur actions ;
 - a. Options sur actions d'une société étrangère ;
 9. Revenus imposables distinctement
 - a. Pécule de vacances anticipé ;

⁵ Voir l'arrêté royal du 5 décembre 1986 *réglant l'accès au Registre national des personnes physiques dans le chef des organismes d'intérêt public relevant du Ministère de la Prévoyance sociale.*

- b. Arriérés (toutes catégories) ;
- c. Indemnités de dédit et de reclassement (toutes) ;
- 10. Avantages non récurrents liés aux résultats (tous) ;
- 11. Timbres intempéries ;
- 12. Rémunérations imposables à 33% (travailleurs occasionnels dans le secteur horeca) ;
- 13. Rémunérations perçues par des sportifs pour l'exercice de leurs activités sportives (rémunérations, pécule de vacances anticipé, arriérés, indemnités de dédit) ;
- 14. Rémunérations obtenues par des arbitres de compétitions sportives pour leurs prestations arbitrales, ou par des formateurs, des entraîneurs et des accompagnateurs pour leur activité au profit de sportifs (rémunérations, pécule de vacances anticipé, arriérés, indemnités de dédit) ;
- 15. PC privé - montant de l'intervention de l'employeur ;
- 16. Intervention dans les frais de déplacement (aussi bien fractionnée que totale) ;
- 17. Rémunération sous la forme de retenues pour pension complémentaire ;
- 18. Heures supplémentaires qui donnent droit à un sursalaire ;
- 19. Précompte professionnel ;
- 20. Bonus à l'emploi ;

b) Les données figurant sur la fiche 281.20 – Rémunérations des dirigeants d'entreprise Il s'agit concrètement des données suivantes :

- 1. Année à laquelle la fiche se rapporte ;
- 2. Numéro de la fiche ;
- 3. Date de l'entrée ;
- 4. Date de la sortie ;
- 5. Débiteur des revenus ;
- 6. Numéro national du bénéficiaire des revenus s'il est domicilié en Belgique. Revenus imposables ou attribués à des résidents ;
- 7. Rémunérations
 - a. Rémunérations ;
 - b. Avantages de toute nature (+ spécifications éventuelles) ;
 - c. Timbres de fidélité ;
 - d. Total des rémunérations ;
 - e. Autres rémunérations ;
- 8. Véhicule mis à disposition : nombre de kilomètres ;
- 9. Options sur actions
 - a. Options sur actions d'une société étrangère ;

10. Quotité du loyer et des avantages locatifs à considérer comme rémunérations (toutes les données) ;
11. Revenus imposables distinctement
 - a. Pécule de vacances anticipé ;
 - b. Arriérés (toutes catégories) ;
 - c. Indemnités de dédit et de reclassement (toutes) ;
12. Avantages non récurrents liés aux résultats (tous) ;
13. Rémunération sous la forme de retenues pour pension complémentaire ;
14. Précompte professionnel ;
15. Rémunérations de dirigeants d'entreprise occupés dans le cadre d'un contrat de travail ;
16. Bonus à l'emploi.

c) Les données figurant sur la fiche 281.50 – Commissions, courtages, ristournes, vacations, honoraires et autres avantages de toute nature.

Il s'agit concrètement des données suivantes :

1. Numéro de la fiche ;
2. Année à laquelle la fiche se rapporte ;
3. Débiteur des revenus (toutes les données) ;
4. Bénéficiaire des revenus (toutes les données)
 - a. Numéro d'entreprise ;
 - b. Profession exercée ;
 - c. Numéro national (s'il est connu) ;
 - d. Numéro d'identification fiscal à l'étranger (s'il est connu) ;
 - e. Date de naissance (si elle est connue) ;
5. Données relatives à la nature des commissions, honoraires, ...
 - a. Montant des commissions, courtages, ristournes commerciales, ... ;
 - b. Montant des honoraires ou vacations ;
 - c. Montant + nature des "avantages de toute nature" ;
 - d. Montant des "frais exposés pour compte du bénéficiaire" ;
 - e. Total ;
6. Indemnités versées à des sportifs pour leurs prestations sportives ;
7. Indemnité versée à des formateurs, entraîneurs et accompagnateurs pour leur activité au profit de sportifs ;
8. Montant réellement payé au cours de l'année à laquelle la fiche se rapporte.

21. Le demandeur estime que la réclamation des données précitées est adéquate, pertinente et non excessive parce que les données sont demandées dans le cadre d'un projet test en vue de limiter les risques de fraude. La détection de ces risques nécessite selon lui que les données susmentionnées soient analysées à grande échelle.
22. Le Comité considère que les données demandées répondent effectivement à l'article 4, § 1, 3° de la LVP, vu les finalités décrites au point 9.

2.2. Délai de conservation des données

23. Dans la demande, il est précisé ce qui suit concernant le délai de conservation : *"L'écriture du code et le développement du modèle prendront approximativement six mois. Si par manque de temps ou en raison de circonstances imprévues, le modèle n'est pas encore prêt dans les 6 mois, l'ONSS en informera le Comité et sollicitera éventuellement une prolongation"*. [Traduction libre réalisée par le Secrétariat de la Commission vie privée en l'absence de traduction officielle]
24. Le Comité estime que si les finalités de test telles que visées au point 9 sont déjà atteintes avant l'expiration de ce délai de six mois, les données devront être détruites avant le terme de ce délai, à savoir dès que les finalités de test sont réalisées.

2.3. Fréquence de l'accès et durée de l'autorisation

25. En ce qui concerne la fréquence de l'accès et la durée de l'autorisation, le demandeur indique ce qui suit : *"Dans un premier temps, l'ONSS ne souhaite qu'une communication unique de données de test pour la mise en œuvre de ce test. Si toutefois les données de test reçues présentent des imprécisions/imperfections (par exemple : métadonnées manquantes, données incomplètes, données impossibles à interpréter, ...), nous n'excluons pas de demander des renseignements ou des données complémentaires. (...) L'écriture du code et le développement du modèle prendront approximativement six mois."* [Traduction libre réalisée par le Secrétariat de la Commission vie privée en l'absence de traduction officielle]
26. Le Comité y consent.

2.4. Destinataires et/ou tiers auxquels des données sont communiquées

27. Seule un groupe très restreint (une dizaine de personnes) de collaborateurs du demandeur et de son sous-traitant auront accès aux données demandées.
28. À la lumière de l'article 4, § 1, 3^o de la LVP, le Comité ne voit aucune objection au fait que les personnes susmentionnées aient accès aux données à caractère personnel en question,
- à condition qu'elles n'utilisent cet accès que dans les limites des tâches et des compétences qui leur ont été attribuées par la réglementation ou par le contrat visé à l'article 16, § 1 de la LVP et
 - uniquement en vue des finalités décrites au point 9.

3. PRINCIPE DE TRANSPARENCE

29. La LVP prévoit qu'un traitement de données loyal est un traitement qui se fait de manière transparente. À cet égard, le demandeur précise ce qui suit : *"En cas d'approbation, l'autorisation sera publiée sur le site Internet de l'ONSS. Les autorisations émises par les différents comités sectoriels compétents sont également publiées sur le site Internet du SPF Finances."* [Traduction libre réalisée par le Secrétariat de la Commission vie privée en l'absence de traduction officielle]
30. Le Comité en prend acte et estime que ces mesures sont adéquates, notamment vu le fait qu'il ne s'agit que d'un projet test ne pouvant avoir aucune conséquence directe pour les personnes concernées (voir le point 9)⁶.

4. SÉCURITÉ

4.1. Au niveau du demandeur

31. Le demandeur fait partie du réseau de la sécurité sociale et est dès lors soumis à l'arrêté royal du 12 août 1993 *relatif à l'organisation de la sécurité de l'information dans les institutions de sécurité sociale*. Cela signifie qu'il dispose :
- d'un conseiller en sécurité de l'information dont la désignation a été soumise au Comité sectoriel de la Sécurité Sociale et de la Santé ;

⁶ À titre complémentaire, on peut également se référer à l'arrêté royal du 11 mars 2015 *portant exécution de l'article 3, § 5, 3^o de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, M.B., 25 mars 2015.

➤ d'un plan de sécurité mentionnant tous les moyens nécessaires à son exécution.

32. Les mesures de sécurité prises par le demandeur peuvent donc être qualifiées d'adéquates.

33. Le demandeur recourt également à un sous-traitant. Le Comité rappelle que dans de tels cas, la LVP impose au responsable du traitement de définir sa relation avec le sous-traitant dans un contrat qui répond aux exigences de l'article 16, § 1 de la LVP.

4.2. Au niveau du SPF Finances

34. En ce qui concerne le SPF Finances, le Comité n'a pas de remarque particulière à ce sujet, étant donné que ces éléments ont déjà fait l'objet d'une évaluation dans d'autres délibérations du Comité.

PAR CES MOTIFS,

le Comité

1° autorise à titre exceptionnel⁷ le demandeur et le SPF Finances à réaliser les traitements de données visés dans la demande d'autorisation ;

2° décide que la présente autorisation est valable si et aussi longtemps que les conditions de la présente délibération sont respectées ; En particulier,

- les données communiquées peuvent uniquement être utilisées en vue des finalités de test visées au point 9 et
- les données doivent être détruites dès que les finalités de test visées au point 9 sont réalisées et en tout cas au plus tard après six mois (sauf prolongation de ce délai par le Comité).

⁷ Vu qu'il s'agit ici d'un projet test bien délimité (voir le point 4) qui s'inscrit dans le cadre des missions légales générales du demandeur et qui n'aura pas de conséquences pour les personnes concernées, le Comité ne s'oppose exceptionnellement pas à ce que ce data mining/data matching soit réalisé sans fondement légal explicite, et ce en attendant que le demandeur prépare la base légale explicite y afférente (voir les points 2-3).

3° décide qu'il se réserve le droit, le cas échéant, de contrôler régulièrement l'application effective et durable de mesures techniques et organisationnelles conformes à l'état de la technique et de nature à couvrir adéquatement les risques. À cet égard, le Comité ordonne aux parties de lui communiquer tout changement pertinent dans la sécurité des traitements autorisés.

L'Administrateur f.f.,



An Machtens



Le Président,



Stefan Verschuere