MARCHE PUBLIC DE SERVICES

MARCHE P2619-AOO-DIFIS

TRAITEMENT DES OPERATIONS BANCAIRES ET FOURNITURE DE SERVICES BANCAIRES ASSOCIES POUR LES ORGANISMES DE L'ASSURANCE RETRAITE

ANNEXE 2 AU CCAP

relative à la PROTECTION DES DONNEES A CARACTERE PERSONNEL

Dans le cadre du présent marché, les parties prenantes aux opérations de traitement s'engagent à respecter la réglementation en vigueur applicable aux traitements de données à caractère personnel et, en particulier :

- Le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, dit « Règlement général sur la protection des données », ci-après « RGPD » ;
- La Loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;
- Le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 susmentionnée ;

La Cnav et/ou les organismes de sécurité sociale, et le titulaire sont responsables sur le périmètre de leurs activités de traitement respectives.

La Cnav et/ou les organismes de sécurité sociale et le titulaire sont qualifiés, selon les opérations de traitement, de fournisseur des données, responsable du traitement des données jusqu'à la réception des données par le destinataire, ou destinataire des données, responsable du traitement des données collectées auprès du fournisseur.

Article I - CARACTERISTIQUES DU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

La ou les **finalité(s) du traitement** sont :
Le traitement des opérations bancaires des organismes de sécurité sociale visés
La fourniture aux organismes de sécurité sociale de services bancaires associés

Les **opérations de traitement** réalisées sur les données à caractère personnel sont :

La collecte,
La conservation,
L'échange de fichiers ou d'informations,
L'utilisation des données à des fins de paiement.

Les **catégories de personnes concernées** sont les bénéficiaires des prestations et aides, les agents des organismes, les fournisseurs.

Les **catégories de données traitées** sont :

Catégories des données	Données à caractère personnel
Identification Exemples : *Nom, prénom, adresse, numéro de téléphone, identifiant, photo, enregistrement sonore, état civil, identité, identité conjoint, identité enfants, sexes, dates de naissance, nationalité, …*	Nom et prénoms
Coordonnées de contact Exemples : *Adresse postale, adresse mail, téléphone fixe, téléphone portable, …*	Adresse postale
Vie personnelle Exemples : *Situation maritale, nombre d'enfants ou de personnes âgées à charge, habitudes de vie, hobbys, …*	NC

Vie professionnelle Exemples : *Profession, employeur, CV, diplôme, formation, distinction, direction, UO, EAEA/EP, numéro d'agent, coefficient, nature du document contractuel, …*	NC
Information d'ordre économique et financier Exemples : *Coordonnées bancaires, RIB, revenue, situation fiscale, pension de retraite, pension de réversion, aides sociales, aides au logement, …*	Coordonnées bancaires
Données de connexions et traçabilité Exemples : *Log, horodatage, adresse IP, traçabilité des actions, journaux d'évènements, cookies fonctionnels, …*	NC
Données de localisation Exemples : *Données GPS, badge, …*	NC
Autres Exemples : *Zones de commentaires libres, bloc-notes, …*	
Données particulières et sensibles *Le niveau de sécurité technique et organisationnel doit être adapté à la sensibilité des données sous-traitées.*	
Identifiants nationaux Exemples : *NIR, NIR d'attente (NIA), …*	NC
Santé, biométrie et génétique Exemples : *Handicap, analyses, forme physique, pathologies, …*	NC
Vie et orientation sexuelle Exemples : *Homosexuel, bisexuel, pratiques sexuelles, …*	NC
Infractions, condamnations ou mesure de sûreté Exemples : *Délits, fraudes, dépôts de plainte, casier judiciaire, jugements, contraventions, …*	NC
Origine raciale ou ethnique Exemples : *Couleurs de peau, traditions, …*	NC
Opinions politiques, philosophiques, convictions religieuses ou appartenance syndicale	NC

Les données à caractère personnel traitées et nécessaires à l'exécution du présent marché, sont transmises par la Cnav et/ou les organismes de sécurité sociale à le titulaire en vue du traitement des opérations bancaires. A cet effet, le titulaire traite les données relatives aux traitements des règlements : nom du bénéficiaire, adresse du bénéficiaire, coordonnées bancaires du bénéficiaire.

Les durées de conservation des données sont gérées comme précisé ci-dessous :

- La Cnav et/ou les organismes de sécurité sociale ne conservent pas les données communiquées plus que nécessaire Ils détruisent leurs copies une fois la confirmation que les données ont bien été réceptionnées et qu'elles sont validées par l'organisme destinataire ou au terme du délai déterminé dans la convention par les parties, sauf dans des cas particuliers de requêtes répétitives ou dépendant du précédent envoi qui justifient une conservation plus longue du fichier.

- Le titulaire destinataire des données ne conserve pas les données communiquées plus que nécessaire à leur traitement Il détruit les copies de données une fois la finalité réalisée. Les données à caractère personnel intégrées dans son SI doivent être conservées pendant une durée proportionnée et limitée au regard des finalités pour lesquelles elles sont traitées. Elles 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, telles que la pseudonymisation ou l'anonymisation.

Article II - QUALIFICATION DES RESPONSABILITES SUR LA PROTECTION DES DONNEES

La Cnav et/ou les organismes de sécurité sociale, et le titulaire sont responsables sur le périmètre de leurs activités de traitement respectives

Ils sont qualifiés, selon les opérations de traitement, de fournisseur des données, responsable du traitement des données jusqu'à la réception des données par le destinataire, ou destinataire des données, responsable du traitement des données collectées auprès du fournisseur.

Le fournisseur des données est responsable de :

- La vérification de la base légale fondant la communication des données au destinataire,
- La vérification de la minimisation des données communiquées au regard des finalités poursuivies par le destinataire,
- La sécurité des données dans son système d'information (recours à des outils d'accès, d'extraction, de transfert et d'hébergement sécurisés pour assurer la confidentialité et l'intégrité des données),
- La sécurité de la communication des données vers le destinataire,
- La qualité des données communiquées,
- La gestion des modalités de conservation (support, archivage, anonymisation ou purge) et de la durée de conservation des fichiers de données constitués et conservés dans son système d'information pour leur communication, le cas échéant.

Le destinataire, en tant que responsable du traitement des données, est responsable de :

- La détermination des finalités de la collecte des données auprès du fournisseur,
- La détermination de la base de licéité fondant la communication des données par le fournisseur,
- La minimisation des données collectées auprès du fournisseur,
- La sécurité des données dans son système d'information (recours à des outils d'accès, d'extraction, de transfert et d'hébergement sécurisés pour assurer la confidentialité et l'intégrité des données),

- La mise en conformité à la réglementation en vigueur applicable aux traitements de données à caractère personnel des traitements des données collectées auprès du fournisseur, y compris aux textes de loi et réglementaires (décrets, arrêtés) encadrant la création et la mise en œuvre de traitements ou de référentiels,
- L'application des droits des personnes concernées sur les données collectées dans le cadre de ses traitements,
- La gestion des modalités de conservation (support, archivage, anonymisation ou purge) et de la durée de conservation des données collectées dans son système d'information,
- La gestion des violations des données collectées dans son système d'information.

Article III - ENGAGEMENTS SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

L'ensemble des parties prenantes aux opérations de traitement s'engagent à :

- Traiter les données pour la ou les finalité(s) compatibles, à moins que la personne concernée ait donné son consentement ou que le traitement ultérieur soit fondé sur le droit de l'Union ou le droit d'un État membre ; 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 ;
- Traiter les données conformément aux textes réglementaires (décrets, arrêtés) encadrant la création et la mise en œuvre de traitements ou de référentiels mutualisés pour plusieurs organismes de la sphère de la protection sociale, le cas échéant ;
- Veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent document contractuel :
  - ✓ S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
  - ✓ Reçoivent la formation nécessaire en matière de protection des données à caractère personnel ;
- Prendre toutes les mesures requises en vertu de l'article 32 du RGPD relatif à la sécurité du traitement et en adéquation avec la sensibilité des données ;
- Assurer la sécurité des flux de données et à utiliser des outils d'échange sécurisés ;
- S'assurer que tous les systèmes, les applications, les services et les produits utilisés dans le cadre des opérations de traitement de données à caractère personnel sont conformes à la réglementation sur la protection des données et intègrent les principes de protection des données dès la conception et par défaut ;
- Informer l'autre Partie en cas de réception d'une plainte, un avis, une communication ou une mise en demeure d'une Autorité de régulation ou de contrôle qui concerne directement ou indirectement les opérations de traitement intervenant dans le périmètre de leur relation contractuelle ou leur non-conformité à la réglementation sur la protection des données à caractère personnel ;
- Conserver les données pendant une durée n'excédant pas celle nécessaire au regard de la ou les finalité(s) pour lesquelles elles sont traitées ;

- En cas de recours à un sous-traitant pour la mise en œuvre des opérations de traitement intervenant dans le périmètre de leur relation contractuelle, s'assurer que ce dernier, ainsi que ses potentiels sous-traitants ultérieurs, présentent le même niveau de garantie pour assurer la protection des données et en informent l'autre Partie. La Partie concernée demeure pleinement responsable devant l'autre Partie de l'exécution par ce sous-traitant et leurs sous-traitants de leurs obligations ;
- S'informer mutuellement lorsque, selon elles, une opération de traitement constitue une violation du droit à la protection des données à caractère personnel.

Article IV - APPLICATION DES DROITS DES PERSONNES CONCERNEES SUR LEURS DONNEES

L'ensemble des parties prenantes aux opérations de traitement répondent à l'exercice des droits des personnes sur le périmètre de leurs opérations de traitement, tel que défini ci-dessus notamment :

- Informent, les personnes concernées sur les caractéristiques des opérations de traitement de données, conformément aux articles 12, 13 et 14 du RGPD ;
- Assurent la gestion et l'effectivité des droits des personnes concernées, conformément à l'article 12 du RGPD, et pour les droits énumérés aux articles 15 à 23 du RGPD, le cas échéant.

Elles se coordonnent par l'intermédiaire de leurs Délégués à la protection des données ou de leurs référents sur la protection des données autant que de besoin et dans la mesure du possible pour toute demande d'exercice de droits présentant un risque pour les droits et libertés des personnes concernées ou en cas de risque de plainte.

Article V - NOTIFICATION ET COMMUNICATION D'UNE VIOLATION DE DONNEES A CARACTERE PERSONNEL

L'ensemble des parties prenantes aux opérations de traitement s'informent mutuellement de toute violation de données à caractère personnel réelle ou potentielle, accidentelle ou non, intervenant dans le périmètre de leur relation contractuelle, dans les 24 heures après en avoir pris connaissance, en l'adressant au Délégué à la protection des données concerné.

Cette information doit être vérifiée et accompagnée de toute documentation utile. La description de la violation de données à caractère personnel comprend la nature de la violation, les catégories de personnes concernées, le nombre approximatif de personnes concernées par la violation, la description des conséquences probables de la violation et les mesures prises pour y remédier.

La notification de la violation de données à l'autorité de contrôle, dans les 72 heures après en avoir pris connaissance, est déterminée et réalisée par le fournisseur des données, lorsque la violation a lieu lors du transfert des données, et par le destinataire, lorsque la violation a lieu suite à sa réception des données.

La partie concernée détermine s'il est nécessaire de réaliser une communication aux personnes concernées. Elle peut demander le concours de l'autre Partie autant que de besoin.

La partie concernée par la violation de données à caractère personnel prend toutes les mesures nécessaires pour remédier à la violation, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Les parties restent joignables directement jusqu'à la résolution de la violation de données.