Protocole de traitement des données à caractère personnel relatif au registre d'affiliation

ENTRE

Les caisses d'allocations familiales qui fournissent les données faisant l'objet du présent protocole :

Caisse d'allocations familiales Infino Brussels vzw, Tervurenlaan 43, 1040 Brussel, numéro BCE 0727.421.608, représentée par Mme Agnes Hertogs, CEO ;

Caisse d'allocations familiales Parentia Brussels vzw, Kartuizerstraat 45, 1000 Brussel numéro BCE 0726.908.991, représentée par Mme Martine Becquevort, CEO ;

Caisse d'allocations familiales KidsLife Brussels vzw, numéro BCE 0426.917.586, Sint-Clarastraat 48 bis, 8000 Brugge, représentée par Mr Van Truong Son Hong, CEO ad interim ;

Caisse d'allocations familiales Brussels Family, Rue Vésale 31, 1000 Brussel, numéro BCE 409.080.771, représentée par Mr Alex Verheyden Président ;

dénommées ci-après « **Organismes d'allocations familiales** »

ET

L'Office bicommunautaire de la santé, de l'aide aux personnes et des prestations familiales - ci-après dénommé Iriscare - Organisme d'intérêt public bicommunautaire (OIP) et destinataire des données faisant l'objet du présent protocole :

Établi à 1040 Bruxelles, rue Belliard 71/2, numéro BCE 0696.977.167, représenté par Mme Tania Dekens, Fonctionnaire dirigeant d'Iriscare ;

dénommé ci-après « **Iriscare** »

Les Organismes d'allocations familiales et Iriscare sont désignés ensemble comme les « **Parties** » ou individuellement comme la « **Partie** ».

Les Parties ont convenu ce qui suit :

1. Définitions

Conformément à l'article 4 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) lu ensemble avec l'article 5 de la loi du 30 juillet

2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, dans le cadre du présent protocole, on entend par :

- « Destinataire » : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement;

- « Données à caractère personnel » : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

- « Traitement » : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou à des ensemble de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

- « Responsable du traitement » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement. Lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'union ou le droit d'un état membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'union ou par le droit d'un état membre;

- « Sous-traitant » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

- « Tiers » : une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel;

- « Violation de données à caractère personnel », une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ;

En outre, dans le cadre de l'application du présent protocole on entend par :

- « Finalité » : l'objectif principal de l'utilisation de données à caractère personnel.

2. Contexte

Suite à la 6ème Réforme de l'Etat, la matière allocations familiales a été régionalisée. Les conditions et modalités d'exercice du droit aux prestations familiales pour les enfants relevant de la compétence de la Commission communautaire commune sont fixées par l'article 23, troisième alinéa, 6°, de la Constitution. Cette matière est désormais encadrée par :

- L'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales ;
- L'ordonnance du 25 avril 2019 réglant l'octroi des prestations familiales.

Les tâches de l'Institution publique de sécurité sociale compétente au niveau fédéral, l'Agence Fédérale des Allocations Familiales "FAMIFED", ont en ce qui concerne les compétences de la Commission communautaire commune, été transférées à Iriscare. Aux fins du présent protocole, Iriscare agit en sa qualité d'autorité de contrôle au sens de l'article 35 de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales et dans le cadre de la réalisation d'études statistiques dans le cadre des missions mentionnées à l'article 28, § 1er, de l'ordonnance du 23 mars 2017 portant création de l'Office bicommunautaire de la santé, de l'aide aux personnes et des prestations familiales.

Les ordonnances précitées du 23 mars 2017, 4 avril 2019 et 25 avril 2019 encadrent désormais la matière des prestations familiales. Celles-ci fixent :

- Les conditions d'octroi et de paiement des prestations familiales;
- Les compétences respectives des organes de gestion et de contrôle des prestations familiales.

Les Organismes d'allocations familiales gèrent les prestations familiales sous le contrôle d'Iriscare et ont notamment pour missions de collecter les données nécessaires à la réalisation de ses missions à savoir :

- L'instruction des demandes relatives aux prestations familiales ;
- La vérification que les allocataires remplissent les conditions d'octroi des prestations familiales posées par les textes légaux et réglementaires ;
- Le paiement des prestations familiales endéans les délais posés par les textes ;

En vertu de l'article 4, § 1er, 5° de l'ordonnance du 23 mars 2017 portant sur la création de l'Office bicommunautaire de la santé, de l'aide aux personnes et des prestations familiales, Iriscare, organisme d'intérêt public bicommunautaire (OIP), exerce ses missions dans la matière des prestations familiales.
A ce titre, Iriscare, demande aux organismes d'allocations familiales bruxelloises de lui fournir les données telles que déterminées par l'article 26/1, § 3, de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales, en vue de la mise en place, la tenue et l'utilisation d'un registre concernant l'affiliation des allocataires auprès des organismes d'allocation familiales.
La Cocom a fait adopter une modification de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des allocations familiales en vue de créer un Registre des Affiliations dont l'objectif est de garantir que les règles relatives à l'affiliation des allocataires auprès d'un Organisme d'allocations familiales, telles que ces règles sont prévues à l'article 26 de l'ordonnance du 4 avril 2019, puissent être correctement appliquées par le circuit de paiement.

Le Registre des affiliations :

- Côté Organismes d'allocations familiales : permet lorsqu'une demande est introduite auprès d'un organisme d'allocation familiales auprès duquel une demande est introduite, de vérifier que l'allocataire n'est pas affilié auprès d'un autre organisme

- Côté Iriscare et dans le cadre de l'application de ce protocole : (a) de contrôler via son Service d'Inspection que les règles d'affiliation dans le circuit de paiement ont été respectées; (b) de réaliser des études statistiques dans le cadre des missions mentionnées à l'article 28, § 1er, de l'ordonnance du 23 mars 2017 portant création de l'Office bicommunautaire de la santé, de l'aide aux personnes et des prestations familiales.

A ce titre, Iriscare sera amené à demander aux Organismes d'allocations familiales bruxellois de lui fournir les données telles que déterminées par l'article 26/1, § 3, de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales, en vue de la mise en place, la tenue et l'utilisation du Registre des affiliations.
Les données à caractère personnel étant collectées par les Organismes d'allocations familiales auprès des personnes physiques concernées par les traitements, Iriscare et les Organismes d'allocations familiales sont amenés à conclure un protocole de transmission des données en vue de leur traitement par Iriscare conformément aux finalités décrites dans l'ordonnance modifiée du 4 avril 2019. Ce protocole sera publié sur les sites respectifs d'Iriscare et des Organismes d'allocations familiales afin de répondre à leur obligation de transparence telle que prévue par le Règlement EU 2016/679 du 27 avril 2016 du Parlement et du Conseil 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.

En vue de la constitution de la base de données "Registre des affiliations" et de la réalisation des traitements décrits ci-après, le responsable de traitement ultérieur précise :

- Avoir soumis pour avis le projet d'ordonnance modifiant l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales à l'Autorité de Protection des Données et s'être conformé intégralement aux observations de cette l'Autorité dans son avis N°189/2021 du 25 octobre 2021 ;
- Avoir soumis au Conseil d'Etat le projet précité, et s'être conformé intégralement aux remarques du Conseil;
- L'ordonnance du 24 décembre 2021, publiée au Moniteur Belge du 21 janvier 2022, a inséré dans l'ordonnance du 4 avril 2019 un article 26/1 portant création d'un registre d'affiliation.

3. Identification des Responsables du traitement et Data Protection Officer (DPO)

3.1. Responsables du Traitement

Dans le cadre de la communication des données visées par le présent protocole, les Organismes d'allocations familiales et Iriscare agissent en qualité de responsables du traitement distincts, à savoir :

- Les Organismes d'allocations familiales, responsables de traitement initiaux, transmettent à Iriscare les données à caractère personnel reprises à l'article 26/1 §3 pour les finalités visées au §2 du même article de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales;
- Iriscare est le responsable de traitement ultérieur des données à caractère personnel qu'il reçoit des Organismes d'allocations familiales et les traite en vue de la mise en place, la tenue et l'utilisation d'un registre des affiliations en son sein.

3.2. Data Protection Officer

Data Protection Officer de la Caisse d'allocations familiales Infino, e-mail : dpo@infino.be

Data Protection Officer de la Caisse d'allocations familiales Parentia Brussels, e-mail : privacy@parentia.be

Data Protection Officer de la Caisse d'allocations familiales KidsLife, e-mail : DPO@Kidslife.be

Data Protection Officer de la Caisse d'allocations familiales BrusselsFamily, e-mail : DPO@brusselsfamily.be

Data Protection Officer d'Iriscare, e-mail : protectiondonnees@iriscare.brussels

4. Objet du protocole

Le protocole est conclu entre le responsable du traitement ultérieur (Iriscare) et les responsables du traitement initial (les Organismes d'allocations familiales) en vertu de l'article 194 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

Les données constituant la base de données «Registre des affiliations» n'ayant pas été collectées par Iriscare auprès des allocataires mais par les Organismes d'allocations familiales, le présent protocole vise à :

- Informer les personnes concernées des traitements qui seront réalisés par Iriscare ;
- Définir les garanties adéquates en vue de la communication de données à caractère personnel par les Organismes d'allocations familiales ;
- Définir les responsabilités entre les responsables du traitement initiaux et le responsable du traitement ultérieur quant au traitement des données ;
- Permettre l'exercice des droits des personnes concernées auprès des responsables des traitements respectifs.

5. Durée du protocole et entrée en vigueur

Le présent protocole de traitement des données entre les Parties prend effet à la date du 1er janvier 2022 et durera aussi longtemps que le traitement des données est effectué en vue de permettre à Iriscare de poursuivre les finalités listées ci-dessous, au point 7 du présent protocole.

6. Base juridique du traitement des données à caractère personnel

Le traitement des données à caractère personnel qui fait l'objet du présent protocole est licite en ce qu'il est « nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis » (art. 6.1.c), du RGPD) ainsi qu'à l'exécution d'une mission d'intérêt public dont est investi le responsable du traitement (art. 6.1.e), du RGPD).

Le Responsable de traitement ultérieur précise que les bases légales des traitements sont les suivantes:

6.1. <u>Pour Iriscare :</u>

- L'article 4, § 1er, 5°, de l'ordonnance du 23 mars 2017 portant sur la création de l'Office bicommunautaire de la santé, de l'aide aux personnes et des prestations familiales, qui stipule qu'Iriscare exerce les missions qui lui sont confiées par cette ordonnance en diverses matières, dont les prestations familiales ;
- L'article 26/1 de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales ;
- L'arrêté du Collège réuni de la Commission communautaire commune du 22 janvier 2022relatif à l'affiliation de l'allocataire auprès d'un organisme d'allocations familiales ;
- L'article 28, § 1er, de l'ordonnance du 23 mars 2017 portant sur la création de l'Office bicommunautaire de la santé, de l'aide aux personnes et des prestations familiales.

6.2. <u>Pour les Organismes d'allocations familiales :</u>

- L'article 26/1 de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales ;
- L'arrêté du Collège réuni de la Commission communautaire commune du 22 janvier 2022 relatif à l'affiliation de l'allocataire auprès d'un organisme d'allocations familiales.

7. Finalités du traitement des données à caractère personnel

Les finalités pour lesquelles Iriscare sollicite la transmission des données faisant l'objet de traitement sont d'assurer :

- l'application correcte des règles concernant l'affiliation de l'allocataire à un Organisme d'allocations familiales telles que visée à l'article 26/1 de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales ;
- la surveillance et le contrôle administratifs conformément à l'article 35 de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales ;
- la réalisation d'études statistiques dans le cadre des missions mentionnées à l'article 28, § 1er, de l'ordonnance du 23 mars 2017 portant création de l'Office bicommunautaire de la santé, de l'aide aux personnes et des prestations familiales, les données communiquées suite à ces études seront anonymisées.

8. Données à caractère personnel

Les données à caractère personnel traitées sont déterminées par l'article 26/1, § 3, de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales.
Les données à caractère personnel à fournir par les Organismes d'allocations familiales sont les suivantes :

- le numéro d'identification de la sécurité sociale (NISS) de la personne qui fait la demande d'affiliation à l'organisme d'allocations familiales ou de la personne qui est affiliée d'office ;
- la cause de l'affiliation, telle qu'une demande d'allocation au sens de l'article 16, § 2, de l'ordonnance du 25 avril 2019 réglant l'octroi des prestations familiales ou une affiliation d'office ;
- la date de la demande ;
- la date d'affiliation de plein droit ;

- la date à laquelle l'allocataire acquiert sa qualité d'allocataire conformément à l'article 26, § 1er, alinéa 2, de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales ;
- la date à laquelle l'allocation de naissance peut être demandée conformément à l'article 16, § 2, de l'ordonnance du 25 avril 2019 réglant l'octroi des prestations familiales.

9. Personnes concernées par le traitement des données à caractère personnel

Les personnes concernées par le traitement des données à caractère personnel effectué dans le cadre de la mise en place, de la tenue et de l'utilisation du registre sont :

- l'allocataire ;
- le futur allocataire ;
- ou une autre personne physique qui introduit une demande d'affiliation au sens de l'article 26 de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales, en vue notamment, d'obtenir indûment des prestations familiales au moyen d'actes frauduleux ou de déclarations fausses ou intentionnellement incomplètes.

10. Mesures requises dans le domaine de la sécurité des données à caractère personnel

Iriscare confirme que, 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, il a pris les mesures techniques et organisationnelles de sécurité adéquates pour protéger les données à caractère personnel contre tout(e) perte, dommage, destruction, vol, divulgation ou toute autre forme de traitement illicite (article 32 du RGPD). Ces mesures comprennent en toute hypothèse :

- des mesures visant à garantir que seul le personnel autorisé ait accès aux données à caractère personnel pour les finalités poursuivies. L'article 26/1, § 5, de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales, précise les catégories de personnes autorisées à traiter ces données à caractère personnel;
- des mesures visant à protéger les données à caractère personnel contre une destruction non intentionnelle ou illicite, une perte ou une altération non intentionnelle, un stockage, un traitement, un accès ou une divulgation non autorisé(e) ou illicite ;
- des mesures visant à identifier les faiblesses relatives au traitement de données à caractère personnel des systèmes utilisés pour mettre en œuvre les finalités poursuivies.

Ces mesures techniques et organisationnelles sont listées à l'annexe 1 du présent protocole.

La transmission des données susmentionnées par les Organismes d'allocations familiales à Iriscare, compte tenu des mesures de sécurité y attachée, se fera dans une première phase, en un échange unique de listes via le protocole SFTP afin d'initialiser le registre d'affiliation et ensuite dans une seconde phase l'échange se poursuivra via un site web qui sera mis à disposition sur la plateforme Portiris.

11. Analyse d'impact relative à la protection des données (AIPD)

11.1. Conformément à l'article 35 du RGPD, les Parties ont réalisé chacune une AIPD.

11.2. Iriscare a mené une AIPD et il en ressort que les mesures prévues pour respecter les principes fondamentaux de la protection de la vie privée et pour traiter les risques résiduels sur la vie privée des personnes concernées sont jugées acceptables au regard des finalités poursuivies.

12. Databreach

12.1. Conformément aux articles 33 et 34 du RGPD, lorsqu'une Partie prend connaissance ou qu'elle suspecte raisonnablement une violation de données à caractère personnel et s'il est probable que la violation engendre un risque pour les droits et libertés d'une personne concernée, la Partie doit notifier cette violation à l'autorité de contrôle dans les meilleurs délais, et au plus tard 72 heures, après en avoir pris connaissance.

Si la violation de données engendre un risque élevé pour les personnes affectées, ces dernières devraient alors également en être informées et des mesures de protection techniques et organisationnelles efficaces ou d'autres mesures qui garantissent que le risque n'est plus susceptible de se matérialiser doivent être prises.

La Partie dont provient la violation de données notifie l'incident à l'autorité de contrôle et, les cas échéants, à la ou aux personne(s) concernée(s).

12.2. La Partie, en tant que Organismes d'allocations familiales, informera la violation des données à Iriscare en envoyant un courrier électronique au DPO d'Iriscare quand la violation des données a eu lieu lors du transfert des données.

12.3. Iriscare informera également la violation des données aux Organismes d'allocations familiales en envoyant un courrier électronique aux DPO d'Organismes d'allocations familiales quand la violation des données a eu lieu à l'occasion des traitements dont il assume la responsabilité.

12.4. L'obligation d'une Partie de signaler une violation de données ou d'y réagir ne peut être interprétée comme une reconnaissance par cette Partie d'une faute ou d'une responsabilité dans son chef concernant la violation de données.

13. Droits des personnes concernées

13.1. Conformément au Règlement EU 2016/679 et à la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, les personnes concernées par les traitements de leurs données à caractère personnel disposent d'un certain nombre de droits ci-après listés :

- Le droit à l'information;
- Le droit de consultation des données;
- Le droit de rectification des données;
- Le droit à l'effacement des données;
- Le droit à la limitation du traitement des données;
- Le droit de s'opposer à tout moment à un traitement de données;
- Le droit de refuser à ce que les données soient traitées de façon automatique.

13.2. En ce qui concerne le droit à l'information, lequel relève de la responsabilité tant du responsable du traitement initial que du responsable du traitement ultérieur, ce dernier sera

assuré par la publication du présent protocole et de ses Annexes sur chacun des sites internet des parties signataires de manière permanente de telle sorte que les allocataires soient informés des traitements et des conditions de réalisation des traitements réalisés par le responsable du traitement ultérieur.

13.3. L'exercice des autres droits des personnes concernées relatifs aux traitements réalisés par Iriscare seront assumés par le responsable du traitement ultérieur dans les conditions propres aux textes règlementaires applicables auxdits traitements.

13.4. Les responsables du traitement initiaux s'engagent à transférer au responsable du traitement ultérieur les demandes et plaintes qui leur parviendraient concernant les traitements assurés par Iriscare conformément aux dispositions du présent protocole.

14. Transmission de données à caractère personnel à des tiers

Les données à caractère personnel ne seront pas accessibles à des tiers et ne seront pas communiquées à des tiers.

15. Durée de conservation des données à caractère personnel

15.1. Les données transmises dans les termes et conditions du présent protocole et du respect des dispositions relatives légales et règlementaires relatives au Registre des Allocations Familiales seront conservées par Iriscare, conformément aux dispositions de l'article 34, § 2, alinéas 3 et 4, de l'ordonnance du 4 avril 2019, établissant le circuit de paiement des prestations familiales :

- Pendant cinq années à dater du dernier jour du trimestre au cours duquel la demande des prestations familiales a été introduite ou la naissance a eu lieu pour les dossiers relatifs aux demandes de prestations familiales qui n'ont pas donné lieu à un paiement, pour autant que la prescription n'ait pas été interrompue ;
- Pendant sept ans à compter du 31 décembre de l'année au cours de laquelle a lieu le transfert des comptes à la Cour des Comptes, pour les dossiers clôturés relatifs à des demandes de prestations familiales ayant donné lieu à au moins un paiement, pour autant que la prescription n'ait pas été interrompue.

15.2. Dès que le traitement des données à caractère personnel n'est plus nécessaire aux fins pour lesquelles elles ont été collectées, elles sont supprimées une fois pour toutes, en tenant compte des dispositions légales en vigueur.

16. Responsabilités des parties /Respect des obligations légales

Par le présent protocole, les Parties reconnaissent leurs rôles et responsabilités tels que décrits dans ce protocole et s'engagent à respecter toutes les obligations légales qui s'appliquent à elles en tant que responsables du traitement distincts des données à caractère personnel.

17. Transparence

Les Parties s'engagent à publier le présent protocole sur leurs sites web.

18. Droit applicable et litiges

Le présent protocole est exclusivement régi par le droit belge.
Les Parties conviennent qu'en cas de litige ou de difficulté dans l'application du présent protocole, elles chercheront d'abord à se concerter et à coopérer en vue de parvenir à une solution amiable dans les meilleurs délais.
A défaut d'une solution amiable, tous les litiges relatifs à ce protocole de traitement de données seront exclusivement soumis aux tribunaux de l'arrondissement judiciaire de Bruxelles.

Fait à Bruxelles le 28/03/2022, chaque Partie déclare avoir reçu son exemplaire.

_____	_____
Responsable traitement Iriscare	Responsable traitement Infino
Mme Tania Dekens, Fonctionnaire dirigeant	Mme Agnes Hertogs, CEO
_____	_____
Responsable traitement Parentia Brussels	Responsable traitement KidsLife Brussels
Mme Martine Becquevort, CEO	Mr Van Truong Son Hong, CEO ad interim

_____

Responsable traitement Brussels Family

Mr Alex Verheyden, Président

Annexe 1 : <u>Les mesures de sécurité techniques et organisationnelles mises en œuvre par Iriscare en vertu de l'article 32 du RGPD</u>

Iriscare a énuméré toutes les mesures techniques et organisationnelles applicables et mises en œuvre pour assurer la sécurité des données et des systèmes.

• Chiffrement : Le transfert des données des caisses d'allocations familiales vers Iriscare se fait avec le protocole de transfert de fichiers sécurisé (SFTP). La connexion SFTP est établie par un fonds en utilisant son certificat privé unique (RSA 2048 bits). La clé publique est envoyée à Iriscare. La connexion est également protégée par un nom d'utilisateur et un mot de passe propres à chaque caisse.
La clé privée reste en possession de la caisse. Le nom d'utilisateur et le mot de passe se trouvent dans la base de données Keypass, protégée par un mot de passe et accessible uniquement aux administrateurs du système Iriscare. Les mots de passe sont envoyés via des services web sécurisés tels que https://onetimesecret.com/ ou https://password.cronos.be
Les données transmises sont copiées avec un certificat SFTP Iriscare et un nom d'utilisateur/mot de passe du serveur SFTP vers le serveur interne d'Iriscare.

• Cloisonnement des données (par rapport au reste du système d'information) : Les données sont placées dans des dossiers qui ne sont accessibles qu'aux utilisateurs disposant d'un profil déterminé, limité à leurs fonctions et à leurs missions.

• Contrôle des accès logiques : Les profils d'utilisateurs sont définis sur la base des groupes de sécurité et de permission Active Directory. Les utilisateurs doivent s'authentifier avec un mot de passe pour accéder aux applications et aux données d'Iriscare en fonction des groupes AD auxquels ils appartiennent. Une politique de mot de passe est mise en place. Il est prévu qu'en cas de 3 tentatives incorrectes, l'utilisateur est temporairement bloqué.

• Traçabilité : Les journaux des connexions et des transferts sont conservés dans un fichier journal. Aucune donnée concernant le contenu des transferts n'est conservée dans les fichiers journaux. Les données du journal SFTP sont conservées pendant un an au maximum.

• Intégrité des données : Les données originales transmises sont stockées dans un dossier "fichiers sources" en lecture seule afin de pouvoir les récupérer en cas d'erreur de traitement.

• Archivage : Les données seront conservées conformément aux dispositions de l'article 34, §2, alinéas 3 et 4, de l'ordonnance du 4 avril 2019 établissant le circuit de paiement des prestations familiales. Iriscare prendra les mesures nécessaires pour que les délais d'archivage soient respectés conformément à ces dispositions.
Dès que le traitement des données à caractère personnel n'est plus nécessaire aux fins pour lesquelles elles ont été collectées, elles sont supprimées une fois pour toutes, en tenant compte des dispositions légales en vigueur.

• Sécurité de l'exploitation : Les systèmes d'exploitation et les applications des serveurs Linux et Windows sont mis à jour selon un processus standard. Pour Linux, cela se fait avec Red Hat Satellite, pour Windows avec SCCM. Les mises à jour standard sont effectuées deux fois par an, à l'exception des mises à jour de sécurité critiques, qui sont effectuées immédiatement. Toutes les mises à jour

passent par les procédures de déploiement standard : d'abord DEV, puis ACC et enfin les environnements PRD.

• Lutte contre les logiciels malveillants : Tous les postes de travail contiennent un logiciel antivirus, géré de manière centralisée et mis à jour plusieurs fois par jour pour les postes connectés au réseau.

• Gestion des postes de travail : Les postes de travail sont automatiquement sécurisés par un verrouillage d'écran après quelques minutes. Il est conseillé aux utilisateurs de verrouiller manuellement le PC lorsqu'ils quittent le poste de travail.

• Sauvegardes : Les sauvegardes des systèmes et des données de production sont gérées de manière centralisée et stockées dans l'environnement sécurisé G-Cloud (Backup-as-a-Service).

• Maintenance : Les serveurs de production sont des machines virtuelles dont la maintenance et les réparations sont confiées au prestataire de services (Smals ou CIRB). Les seuls serveurs physiques sont les hôtes Windows qui sont pris en charge au niveau matériel par les fournisseurs. Les fournisseurs n'ont pas accès aux logiciels ou aux données sur les serveurs. Les supports de données défectueux sont envoyés dans des centres spécialisés pour y être détruits afin d'effacer définitivement les données qu'ils contiennent.
Si l'accès aux applications ou aux systèmes est nécessaire pour une intervention, il ne sera ouvert et contrôlé qu'à ce moment-là et sous la supervision d'un administrateur système d'Iriscare. Cela peut se faire physiquement dans le bureau ou par le biais d'une session TeamViewer supervisée à distance.

• Sécurité des canaux informatiques (réseaux) : Le traitement a lieu sur le réseau privé d'Iriscare. La sécurité du réseau Iriscare répond aux mêmes exigences de qualité que la sécurité du réseau IAP du G-Cloud.

• Surveillance : Les systèmes et réseaux de production sont surveillés en permanence et en temps réel avec Microsoft SCOM (tableau de bord visuel et alertes par courriel) et PRTG (tableau de bord visuel).

• Contrôle des accès physiques : Les données sont traitées dans les salles de serveurs sécurisées des centres de données IN et UP de Smals et du CIRB. L'accès aux centres de données est strictement réglementé et n'est demandé que par e-mail et uniquement par quelques personnes autorisées (au moins 24 heures à l'avance). L'accès est validé par la gestion des accès des centres de données par retour de mail. Pour l'accès, un badge personnel est activé à la réception du centre de données (à nouveau après vérification de la demande) pour la durée de l'intervention. Toutes les portes d'accès sont verrouillées et le badge ne donne accès qu'aux zones autorisées pour le visiteur.

• Sécurité du matériel : Tous les serveurs sont situés dans des salles sécurisées auxquelles on ne peut accéder qu'avec des badges autorisés. Les utilisateurs doivent verrouiller leur poste de travail avec leur verrou de sécurité personnel. Les données relatives au matériel qui n'est plus utilisé sont supprimées avant d'être remises en circulation. Les données sur le matériel défectueux sont détruites par les services professionnels spécialisés.

• Éloignement des sources de risques : Le centre de données de Smals et du CIRB sont doublement sécurisés (au moyen de deux installations différentes).

• Protection contre les sources de risques non-humaines : Les centres de données où les données sont traitées sont conformes à la norme Tier 3. Les systèmes sont redondants dans deux centres de données afin de minimiser les temps d'arrêt en cas de catastrophe. Les locaux d'Iriscare font l'objet de contrôles réguliers des risques d'incendie. Présence de portes coupe-feu. Iriscare dispose également d'un service de prévention.

• Iriscare a un Data Protection Officer.

• La politique de sécurité d'Iriscare est basée sur les normes de sécurité minimales de la BCSS.

• Gestion des incidents et de violation des données : Il existe un plan de gestion des incidents au sein d'Iriscare. En cas de violation de données à caractère personnel, le Service protection des données est informé dans les brefs délais, une évaluation de la situation est menée et si, suite à cette évaluation, des mesures doivent être prises, celles-ci sont aussitôt appliquées. Lorsque cela est nécessaire, l'Autorité de protection des données est informée de la violation de données dans les 72 heures au plus tard.

Iriscare informe immédiatement les autres responsables de traitement de toute violation des données.

• Le personnel et les collaborateurs d'Iriscare sont soumis à une obligation de confidentialité et au secret professionnel.
