

LETTRE A TOUTES LES CAISSES n° DAJI-2010-474

Direction des Affaires Juridiques et Institutionnelles

CM

Bagnolet, le 23 novembre 2010

Objet : Guichet Unique Virtuel

Madame, Monsieur le Directeur Général,
Madame, Monsieur le Directeur,

Je vous informe de la mise en oeuvre du traitement de données à caractère personnel relatif au Guichet Unique Virtuel.

Ce traitement a pour finalité de permettre aux agents MSA de consulter le dossier d'un adhérent, quelles que soient les MSA qui le gèrent ou l'ont géré.

Ce traitement a été enregistré par le Correspondant Informatique et Libertés sous le numéro CIL 10-11 en date du 05 novembre 2010.

Toutes les caisses de Mutualité Sociale Agricole sont concernées par ce traitement.

Par conséquent, vous trouverez ci-joint copie de la décision de la CCMSA, laquelle devra être signée, puis publiée par voie d'affichage dans les locaux et sur le site internet de chaque caisse; pendant toute la durée du traitement.

Je vous prie d'agréer, Madame, Monsieur le Directeur Général, Madame, Monsieur le Directeur, l'assurance de mes salutations distinguées.

**Signée par la Directrice des Affaires
Juridiques et Institutionnelles**

Agnès CADIOU

Nombre de document(s) annexe(s) : 10

Département «Affaires Juridiques»
Dossier suivi par Catherine MARTINEZ
☎ 01 41 63 70 90
📠 01 41 63 71 15

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Décision portant sur un traitement de données à caractère personnel relatif au Guichet Unique Virtuel

Le Directeur Général de la Caisse Centrale de la Mutualité Sociale Agricole,

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée en dernier lieu par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;

Vu l'article L. 723-11 du code rural ;

Vu le décret n° 2009-1577 du 16 décembre 2009 relatif au Répertoire National Commun de la Protection Sociale ;

Vu le décret 2008-371 du 18 avril 2008 relatif à la coordination de la lutte contre les fraudes et créant une délégation nationale à la lutte contre la fraude ;

Vu l'avis du conseil central d'administration de la Mutualité sociale agricole en date du 7 mai 2009 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés relatif au Répertoire National Commun de la Protection Sociale en date du 30 avril 2009 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés n°1142316 relatif aux services sécurisés Extranet en date du 03/09/2007 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés relatif à l'ensemble des téléprocédures pour simplifier les démarches administratives en date du 03//08/2006 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés n°94062 relatif au fichier d'identification de la Population Agricole en date du 28/06/1994 ;

Vu la décision du Correspondant Informatique et Libertés n° 10-11 en date du 05 novembre 2010, permettant la mise en place du Guichet Unique Virtuel.

décide:

Article 1^{er}

Il est créé au sein des organismes de Mutualité Sociale Agricole (MSA) un traitement automatisé de données à caractère personnel dénommé Guichet Unique Virtuel dont l'objet est de permettre aux agents MSA de consulter le dossier d'un adhérent, quelles que soient les MSA qui le gèrent ou l'ont géré.

Article 2

Les informations concernées par ce traitement sont les suivantes :

- le numéro GUV,
- le numéro NIL,
- le code de gestion caisse
- les motifs de gestion maladie
- les motifs de gestion famille

- les motifs de gestion vieillesse,
- les motifs de gestion accident du travail et maladie professionnelle,
- les motifs de gestion cotisation,
- les motifs de gestion contentieux,
- le code de fin de motif de gestion,
- la date de début d'effet du motif,
- la date de fin d'effet du motif,
- la date de début d'échange de période,
- la date de fin d'échange de période.

Article 3

Les destinataires ou catégories de destinataires habilités à recevoir communication de ces données sont, à raison de leurs attributions respectives :

- la Direction de la Maîtrise d'ouvrage Institutionnelle de la CCMSA,
- la Direction Maîtrise des risques,
- la Direction des Echanges des répertoires et des statistiques de la CCMSA,
- la Direction de la protection sociale de la CCMSA.

Article 4

Conformément aux articles 39 et suivants de la loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés, toute personne peut obtenir communication et, le cas échéant, rectification ou suppression des informations la concernant, en s'adressant au directeur de l'organisme de mutualité sociale agricole dont elle relève.

Article 5

Le Directeur Général de la Caisse Centrale de la Mutualité Sociale Agricole et les Directeurs des organismes de Mutualité Sociale Agricole sont chargés, chacun en ce qui les concerne, de l'exécution de la présente décision.

Fait à Bagnolet, le

Le Directeur Général de la Caisse Centrale
de la Mutualité Sociale Agricole



François GIN

« Le traitement automatisé de données à caractère personnel mis en œuvre par la
est conforme aux dispositions de la présente décision ci-dessus. Ce traitement est placé sous la responsabilité du Directeur de la caisse pour ce qui le concerne.
Le droit d'accès et de rectification des informations à caractère personnel contenues dans ce traitement est ouvert à toutes les personnes physiques concernées par le traitement. Il s'exerce auprès du Directeur de la Caisse ou de l'organisme de MSA. ».

A....., le.....

DECLARATION NORMALE

CIL

**Correspondant
Informatique
et Libertés**

1 type de déclaration

PREMIERE DECLARATION	X
DECLARATION DE MODIFICATION	
Préciser dans ce cas le n° d'enregistrement du traitement que vous souhaitez modifier :	

<p>Cadre réserve au CIL</p> <p>N° d'enregistrement 10-11</p>

2 Déclarant

Statut juridique :	Secteur public <input checked="" type="checkbox"/>	ou Secteur privé
Nom (prénom) ou raison sociale :	Caisse Centrale de Mutualité Sociale Agricole	
Service...	Direction des Affaires Juridiques et Institutionnelles.....	
Adresse	Les mercuriales - 40 avenue Jean Jaurès.....	
Code postal :	93 547 Ville...BAGNOLET CEDEX...	

3 Service ou organisme chargé de la mise en œuvre du traitement (cf annexe 3)

Nom ou Raison Sociale...	Caisse Centrale de Mutualité Sociale Agricole et les Caisses de Mutualité Sociale Agricole
Service.....	

4 Service ou organisme chargé du droit d'accès (cf annexe 4)

Nom ou Raison Sociale	La Caisse de Mutualité Sociale Agricole dont relève l'intéressé
Service.....	
Adresse.....	
Code postal Ville.....

4-1 Mesures prises pour informer les intéressés de leurs droits (cf annexe 4)

	par une mention sur le questionnaire de collecte	X	par affichage
	par la remise d'un document	X	par une mention sur le site internet
	par envoi de courrier		par intranet
	Autres		

Si vous avez coché « Autres », précisez.....
.....

4-2 Moyens permettant d'exercer son droit d'accès (cf annexe 4)

	par un accès en ligne à leur dossier	<input checked="" type="checkbox"/>	par voie postale
	par courrier électronique	<input checked="" type="checkbox"/>	sur place
	Autres.....		
Délai moyen de communication..... 1 mois.....			

5 Contact :

Nom et Prénom **MARTINEZ Catherine**.....
Adresse électronique.. **martinez.catherine@ccmsa.msa.fr**

Fonction... **Juriste**
Téléphone : **01.41.63.70.90**

6 Traitement déclaré (cf annexe 6)

Finalité du traitement : La finalité du Guichet Unique Virtuel est de permettre aux agents MSA de consulter le dossier d'un adhérent, quelles que soient les MSA qui le gèrent ou l'ont géré.

L'objectif du traitement : Le Guichet Unique Virtuel s'appuiera sur des référentiels, afin de :

- assurer le routage vers le ou les systèmes d'information compétents pour traiter le service offert
- réaliser la consolidation et/ou la présentation d'information par des services métier
- permettre la transterritorialité

De plus, le GUV est un élément essentiel d'articulation en vue de couvrir les enjeux institutionnels, en terme :

- de mise à disposition pour les partenaires de la protection sociale d'un portail de services permettant l'échange réciproque d'information
- d'apport aux usagers extranets de la permanence de leurs abonnements et préférences aux services extranet MSA
- d'amélioration, de sécurisation des procédures et de moyens de lutte contre la fraude qui sont mis à disposition des agents MSA par le partage d'informations.

Le nom du logiciel : Guichet Unique Virtuel

Population concernée : La population de la Mutualité Sociale Agricole

7 Transferts d'informations hors de l'Union européenne

Existe-t-il des transferts d'informations hors de l'Union européenne ?

OUI

NON



8 Fonctions de l'application (cf annexe)

1-Routage d'information

2-Consolidation et/ou présentation d'information

3 Transterritorialité (*exemple : les préférences des extranets qui sont communes pour toutes les CMSA lorsque l'adhérent est multi CMSA, et permanentes lorsque l'adhérent change de CMSA*)

4 -

9 Échanges de données

Le traitement a-t-il pour objet l'interconnexion de fichiers :

1 / dont les finalités principales sont différentes ? OUI NON

2 / dont les finalités correspondent à des intérêts publics différents ? OUI NON

10 Sécurités et secrets (cf annexe 10 et 10 bis))

Mettez-vous en place des règles permettant de contrôler l'accès à l'application ? OUI NON

Prenez-vous des dispositions pour protéger votre réseau des intrusions extérieures ? OUI NON

Les données elles-mêmes font-elles l'objet d'une protection particulière (anonymisation, chiffrement...) ? OUI NON

11 Catégories de données (cf annexe 12)

Catégories de données enregistrées


X	A	Données d'identification (noms, prénoms, sexe, initiales, n° s d'ordre, date et lieu de naissance)	I	Moyens de déplacement des personnes
	B	NIR, N° de Sécurité Sociale ou consultation du RNIPP	J	Utilisation des médias et moyens de communication
X	C	Situation familiale	K	Données à caractère personnel faisant apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques, religieuses ou les appartenances syndicales des personnes
	D	Situation militaire	L	Données biométriques
	E	Formation - Diplômes - Distinctions	M	Santé, données génétiques, vie sexuelle
	F	Adresse, caractéristiques du logement	N	Habitudes de vie et comportement
	G	Vie professionnelle	O	Informations en rapport avec la police
X	H	Situation économique et financière	P	Informations relatives aux infractions, condamnations ou mesures de sûreté

Catégories d'informations fournies

12 Catégories des destinataires

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1		X	X					X								
2		X	X					X								
3		X	X					X								
4		X	X					X								
5																
6																
7																
8																
9																
10																

13 Signature du CIL

NOM et Prénom	CADIOU Agnès	Signature	
Date le (JJ/MM/AAAA)	05/11/2010		

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Guichet Unique Virtuel

Annexe 3 : service chargé de la mise en œuvre du traitement

Page 1/1

3.1) service chargé de la mise en œuvre du traitement

Les fichiers d'alimentation du référentiel Guichet Unique Virtuel émanent des systèmes d'information métier régionaux (famille, maladie, vieillesse, entreprise/établissement etc.) et sont envoyés par les centres informatiques (CITI) des Caisses de MSA. Ces fichiers sont réceptionnés par le centre informatique de la Caisse Centrale de Mutualité Sociale Agricole (le CIMAFAP site de Nanterre) afin d'alimenter un référentiel.

Au sein de la Caisse Centrale, plusieurs directions auront accès au référentiel Guichet Unique Virtuel. Il s'agit de :

- La Direction de la Maîtrise d'Ouvrage Institutionnelle via le département gestion centralisée qui est responsable de la maîtrise d'ouvrage centrale du Guichet Unique Virtuel et dont la mission est également d'assurer le bon fonctionnement de l'application ;
- La Direction Maîtrise des Risques qui vise à lutter contre la fraude et à surveiller les actes répréhensibles qui porteraient atteinte aux intérêts financiers de la Mutualité Sociale Agricole ;
- La Direction des Echanges des répertoires et des Statistiques via la Sous Direction des Echanges et des répertoires qui est en charge de la qualité des répertoires ;
- La Direction de la Protection Sociale qui assure la mise en application et le suivi des évolutions législatives.

3.2) intervention d'un sous-traitant

Il n'y a pas d'intervention de sous-traitant sur le projet Guichet Unique Virtuel

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Guichet Unique Virtuel

Annexe 4 : Mesures prises pour faciliter le droit d'accès

Page 1/2

4.1 Modalités générales

La décision sera :

- affichée dans les locaux de chacune des caisses de MSA concernées,
- publiée sur le site intranet ou internet des caisses de MSA concernées.
- publiée sur le site internet de la CCMSA

Dans la mesure où le présent traitement se présente sous la forme d'un dossier national, chacun des Organismes de Mutualité Sociale Agricole concerné par la présente action aura à établir un engagement de conformité sur lequel figurera la mention selon laquelle le traitement effectué au niveau local est conforme au contenu de la demande nationale.

4.2 Droit d'accès

La loi du 6 janvier 1978 reconnaît à toute personne figurant dans un traitement un droit d'accès aux renseignements la concernant (article 39).

Le droit d'accès s'exerce par voie postale auprès de la Direction de la Maîtrise d'Ouvrage Institutionnelle - Département Gestion Centralisée à l'adresse suivante :

Caisse Centrale de Mutualité Sociale Agricole
DMOI- Département Gestion Centralisée
40 rue Jean Jaurès
93547 Bagnolet cedex

Le délai prévu pour satisfaire à une demande de droit d'accès est d'environ 1 mois.

4.3 Droit de rectification

Toute personne peut demander que soient rectifiées, complétées, mise à jour ou effacées les données la concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, l'utilisation, la communication ou la conservation est interdite (article 40 de la loi n°78-17 du 6 janvier 1978).

Le droit de rectification s'exerce dans les mêmes conditions que celles du droit d'accès.

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Guichet Unique Virtuel

Annexe 4 : Mesures prises pour faciliter le droit d'accès (suite)

Page 1/2

4.4 Droit d'opposition

Toute personne physique a le droit de s'opposer pour des motifs légitimes, à ce que des données à caractère personnel la concernant face l'objet d'un traitement. Ce droit ne s'applique pas lorsqu'il répond à une obligation légale (article 38 de la loi n°78-17 du 6 janvier 1978).

Le droit d'opposition s'exerce dans les mêmes conditions que celles du droit d'accès

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Guichet Unique Virtuel

Annexe 6: Finalité principale du traitement

Page 1/2

6.1 Généralités

Deux parties composent le projet Guichet Unique Virtuel :

- La partie routage : Elle traite de la gestion du routage permettant d'assurer la « transterritorialité » pour « les individus » et « entreprises /établissements ».
- La partie Extranet : Elle apporte aux Extranetes la vision de tous les services extranets dont ils bénéficient sans qu'ils soient contraints de devoir accéder à chaque site des CMSA qui ont en charge la gestion de leur dossier.

6.2 Fondements juridiques

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée en dernier lieu par la loi N°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- Article L. 723-11 du code rural qui précise que la Caisse Centrale de la Mutualité Sociale Agricole a notamment pour missions :
 - o « de mettre en œuvre ou de coordonner les actions de contrôle sur le service des prestations afin de détecter les fraudes et les comportements abusifs. Elle peut à ce titre utiliser des traitements automatisés des données relatives au service des prestations.
 - o de mettre en œuvre ou de coordonner des actions de contrôle sur le service des prestations afin de détecter les fraudes et les comportements abusifs. Elle peut requérir la participation des caisses mentionnées à l'article L.723-2. Elle peut à ce titre utiliser des traitements automatisés des données relatives au service des prestations ».
- Décret 2008-371 du 18 avril 2008 relatif à la coordination de la lutte contre les fraudes et créant une délégation nationale à la lutte contre la fraude ;
- Décret n° 2009-1577 du 16 décembre 2009 relatif au Répertoire National Commun de la Protection Sociale ;
- Avis du conseil central d'administration de la Mutualité sociale agricole en date du 7 mai 2009 ;
- Avis de la Commission nationale de l'informatique et des libertés relatif au Répertoire National Commun de la Protection Sociale en date du 30 avril 2009 ;
- Avis de la Commission nationale de l'informatique et des libertés n°1142316 relatif aux services sécurisés Extranet en date du 03/09/2007 ;

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Guichet Unique Virtuel

Annexe 6: Finalité principale du traitement (suite)

Page 2/3

- Avis de la Commission nationale de l'informatique et des libertés relatif à l'ensemble des téléprocédures pour simplifier les démarches administratives en date du 03//08/2006 ;
- Avis de la Commission nationale de l'informatique et des libertés n°94062 relatif au fichier d'identification de la Population Agricole en date du 28/06/1994.

6.3 Objectifs du traitement

L'objectif du guichet unique virtuel est de permettre aux agents MSA de consulter le dossier d'un adhérent, quelles que soient les MSA qui le gèrent ou l'ont géré.

On peut distinguer deux niveaux :

Au niveau local (Caisse de MSA) l'objectif est :

- d'apporter aux agents de l'institution MSA la vision des informations qui concernent l'adhérent quel que soit la ou les CMSA qui gèrent ou ont géré l'adhérent.
- d'échanger des informations intra MSA : Les services d'échange d'information entre CMSA demandent au GUV la localisation des systèmes d'information technique sur la base du motif de gestion associé au service et de l'identifiant sur lequel porte la demande d'information.

Au niveau National (Caisse Centrale de MSA) l'objectif est :

- d'alimenter le RNCPS¹ avec Les Données Centralisées de Rattachement (à l'aide des données « motifs de gestion » de prestation stockées au sein du référentiel GUV)
- répondre aux sollicitations du RNCPS sur les Données Complémentaires de Prestation concernant les assurés du régime agricole quelle que soit la ou les CMSA qui les gèrent (routage d'information vers les systèmes d'information régionaux) ;
- apporter aux fournisseurs de Flux les informations nécessaires à l'éclatement et au transfert du contenu des fichiers en provenance des partenaires lorsqu'ils ne sont pas porteurs de la ou des CMSA de destination.

De plus, plusieurs cas d'usage du Référentiel Guichet Unique Virtuel peuvent être recensés comme :

- INTEROPS² : dans le fonctionnement général de l'Interopérabilité des organismes de la Protection Sociale, le Référentiel GUV est sollicité pour rechercher les systèmes d'information technique. Les systèmes d'information technique permettent de localiser les informations métiers requises par les services offerts aux partenaires.
- Router le contenu de flux : pour les flux qui ne sont pas porteurs de l'identification des Systèmes d'information technique, qui gèrent les éléments composant le flux, le routage du contenu du flux vers les Systèmes d'information technique est effectué en interrogeant le Référentiel GUV avec le

¹ Référentiel National Commun de la Protection Social

² Standard d'Interopérabilité entre les Organismes de la Protection Sociale

motif de gestion et les identifiants des entités à localiser.

6.4 Données à traiter

Pour les individus, toute la population agricole référencée dans les systèmes d'identification régionaux et nationaux est concernée, sauf :

- les populations en attente de gestion,
- les populations extérieures au régime ou à la caisse pour la médecine du travail, pour les élections, pour la complémentaire maladie (...)

Pour les entreprises et les établissements, toutes les entreprises agricoles et établissements agricoles connus par la MSA sont concernés par le référentiel GUV.

Le traitement ne concerne pas de données sensibles telles que :

- Le NIR
- Les données de santé. Présence unique de données médico-administratives.

Deux types de données sont remontés au sein du référentiel :

- des motifs de gestion
- et les dates d'effet associées aux motifs de gestion

Les motifs de gestion, ainsi que les dates d'effet, sont calculés par les systèmes d'information métiers régionaux par rapport à la situation des individus gérés en MSA en tant que prestataire. Les données calculées seront remontées au niveau national pour être stockées dans le référentiel GUV.

Pour les individus, les entreprises et les établissements, les motifs de gestion caractérisent un ensemble ou un sous ensemble de données afin d'en connaître leurs localisations dans les systèmes d'information métiers respectifs. Ils ont été définis en s'appuyant sur des classifications métiers MSA.

Pour plus de détails sur les données, se reporter à l'annexe n°12.

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Référentiel Guichet Unique Virtuel

Annexe 10 : *sécurités et secrets*

Page 1/9

I) **SECURITE DU CENTRE INFORMATIQUE NATIONAL DE LA MSA**

10.1 sécurité physique

Le serveur sur lequel sont hébergés les fichiers de données à caractère personnel est implanté dans un local sécurisé, dont les accès sont contrôlés.

Protection des locaux :

Une seule entrée permet l'accès du personnel au Centre informatique national de la MSA, lequel est gardé 24h/24 et 7j/7 par un agent de surveillance. Toutes les autres entrées ont été condamnées ou transformées en issues de secours et sont gérées en tant que telles, c'est à dire fermées de l'extérieur et dotées de détecteurs d'ouverture dont la gestion est centralisée.

De plus, les locaux techniques sont accessibles au seul personnel habilité du Centre informatique national de la MSA, par zones de sécurité, en fonction des droits dont il dispose. La sécurité de ces zones est assurée par lecture de badges magnétiques.

Contrôles d'accès physiques :

La protection contre les intrusions est assurée comme suit :

Le centre est gardé en permanence (7j/7 et 24h/24) par des agents de surveillance appartenant à une société spécialisée en gardiennage informatique, dont les rondes sont contrôlées par le responsable des services généraux du Centre informatique national de la MSA.

Les agents de sécurité disposent d'écran relais de caméras de surveillance des locaux, des écrans et matériels témoins de la gestion technique centralisée (détection incendie, extinction, climatisation, intrusion), une salle de contrôles et d'alarmes possédant poste de travail et matériels d'impression pour la délivrance de badges aux visiteurs.

Il n'existe pas de transmission d'alarmes à distance vers l'extérieur du bâtiment, mais des alarmes internes centralisées et transmises au poste central de sécurité, géré par un gardien permanent.

Pendant les heures ouvrées (7h/19h du lundi au vendredi), un badge d'identification informatisé est délivré par ces agents à toute personne autre que le personnel appartenant au Centre informatique national de la MSA.

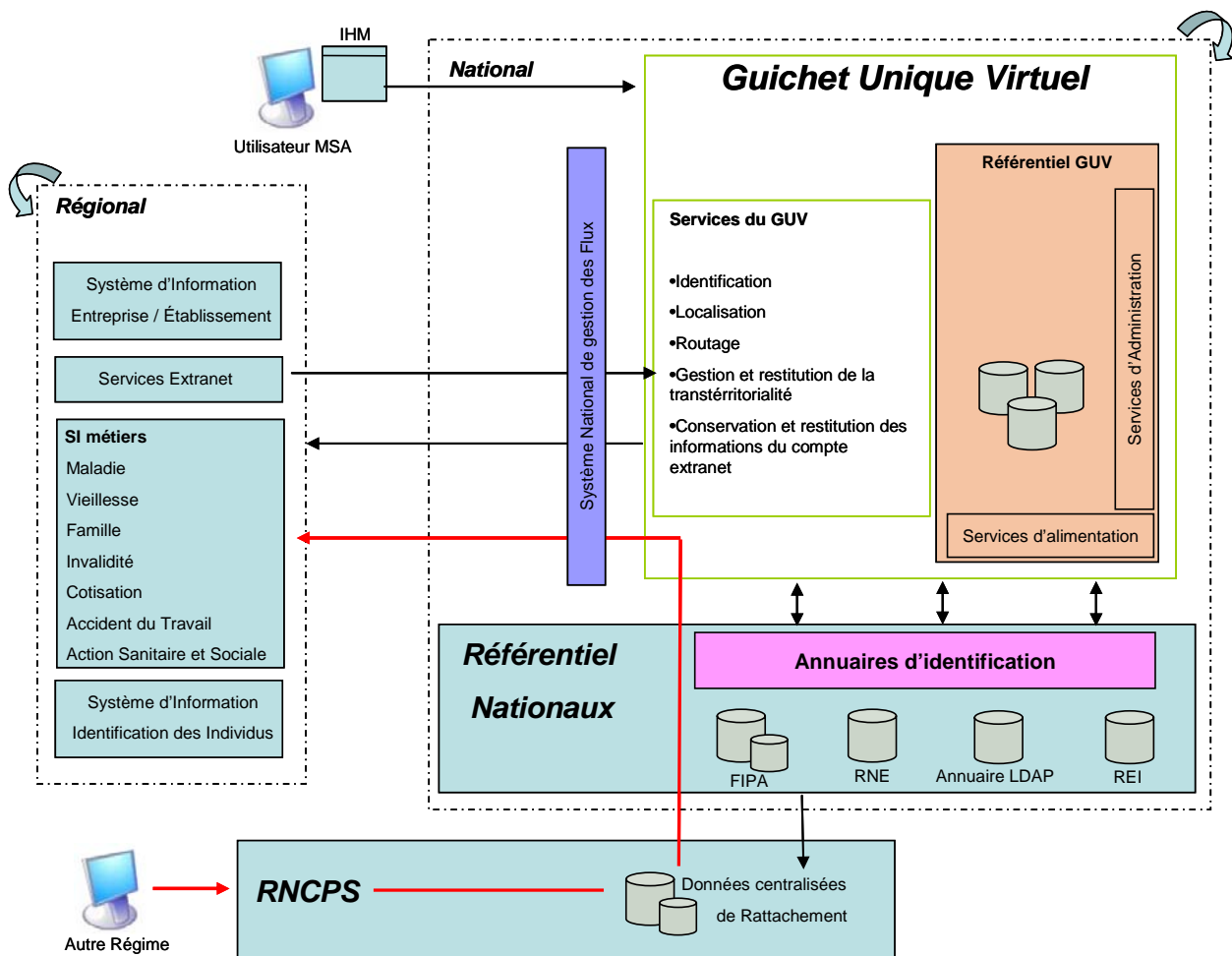
CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Guichet Unique Virtuel

Annexe 8 : Fonctions et caractéristiques techniques

Page 1/3

8.1 Fonctionnalité du traitement



Légende du schéma :

FIPA : Fichier identification de la Population Agricole.

RNE : Référentiel National des entreprises et établissements

REI : Référentiel Environnement Institutionnel. C'est le référentiel dépositaire de l'ensemble des composantes internes (Monde MSA) de l'Institution et de ses partenaires externes et garant de la cohérence des échanges transitant par l'Echelon Central

Annuaire LDAP : C'est un annuaire basé sur le protocole TCP/IP qui permet de partager des informations sur les contacts et des informations sur les assurés ou usagés extranetes.

IHM : Interface Homme/Machine

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Guichet Unique Virtuel

Annexe 8 : Fonctions et caractéristiques techniques (suite)

Page 2/3

Au Niveau régional, il y a génération d'un flux pour les entités de type « Individu » et « Entreprise / Etablissement ».

Deux types de fichier sont constitués au niveau régional en fonction de la population traitée :

1. Un fichier avec les données individus, qui est composé de :
 - ✓ un Numéro Invariant Large (NIL), c'est un numéro interne MSA pour identifier un individu
 - ✓ un code motif de gestion métier (caractérisant un ensemble ou un sous ensemble de données permettant de connaître la localisation des informations recherchées dans les systèmes d'information respectifs)
 - ✓ un code de gestion pour les CMSA propriétaires des données (système d'information technique de la CMSA)
 - ✓ une date de début d'effet du motif
 - ✓ une date de fin d'effet du motif
 - ✓ une date de début d'échange de période
 - ✓ une date de fin d'échange de période
 - ✓ un code de fin du motif de gestion (disparu, décès, fin de gestion et mutation)

2. Un fichier avec les données entreprise / établissement, qui est composé de :
 - ✓ Un numéro entreprise ou un numéro établissement, c'est un numéro interne MSA pour identifier l'entreprise / l'établissement
 - ✓ un code motif de gestion métier
 - ✓ un code de gestion pour les CMSA propriétaires des données
 - ✓ une date de début d'effet du motif
 - ✓ une date de fin d'effet du motif
 - ✓ une date de début d'échange de période
 - ✓ une date de fin d'échange de période
 - ✓ un code de fin du motif de gestion

Au niveau national, le traitement GUV a pour objet pour chaque entité :

- d'identifier l'entité par interrogation de l'Annuaire d'identification via des services.
- de mettre à jour référentiel GUV
- d'incrémenter un numéro d'ordre GUV permettant d'identifier un individu en s'appuyant sur les référentiels nationaux d'identification

Un fichier d'initialisation par caisse de MSA sera généré au niveau régional pour alimenter le référentiel GUV de la population agricole. Ce fichier sera produit une seule fois par chaque caisse de MSA, avant l'enclenchement des traitements d'actualisation du référentiel GUV en temps réel.

La mise à jour en temps réel du référentiel GUV se base sur l'utilisation des faits générateurs / instances produits par les applications métiers au régional.

Au niveau régional, Il y a génération d'un flux périodique ne contenant que les mouvements de mise à jour (se rapportant à une évolution de situation de l'entité par rapport à un précédent envoi) pour un Individu et une Entreprise / Etablissement avec constitution d'un fichier par CMSA.

Il y a « persistance » d'une référence en régional du GUV afin de garder trace des motifs de gestion dans le SI régional pour que les traitements analyseurs puissent déterminer s'il s'agit d'une évolution de situation ou non et ainsi éviter des envois inutiles vers le National.

Les situations envoyées par les traitements en caisse pour mise à jour du référentiel GUV font l'objet d'un retour.

Pour assurer ses fonctions (routage, localisation et identification) le GUV utilise :

- L'annuaire d'identification pour l'identification des entités individu et entreprise/établissement.
- Le Référentiel Environnemental Institutionnel pour obtenir des informations relative au Système d'Information Technique de localisation comme :
 - la dénomination de la CMSA propriétaire du Système d'Information Technique
 - la validité de l'identifiant au Système d'Information Technique

Une Interface Homme / Machine (IHM) permet d'accéder en consultation aux données présentes dans le référentiel GUV. L'accès aux données du référentiel GUV sera limité à :

- ✓ La Direction de la Maîtrise d'Ouvrage Institutionnelle via le département gestion centralisée qui est responsable de la maîtrise d'ouvrage centrale du Guichet Unique Virtuel et assure le bon fonctionnement de l'application.
- ✓ La Direction Maîtrise des Risques qui vise à lutter contre la fraude et à surveiller les actes répréhensibles qui porteraient atteinte aux intérêts financiers de la Mutualité Sociale Agricole.
- ✓ La Direction des Echanges des répertoires et des Statistiques via la Sous Direction des échanges et des répertoires qui est en charge de la qualité des répertoires.
- ✓ La Direction de la Protection Sociale qui assure la mise en application et le suivi des évolutions législatives.

8.2 Caractéristiques techniques

Les traitements sont effectués au niveau régional et national (site informatique de la MSA) sous environnement UNIX.

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Référentiel Guichet Unique Virtuel

Annexe 10 : *sécurités et secrets (suite)*

Page : 2/9

Les personnes de sociétés extérieures devant intervenir sur le site temporairement (ex : travaux de réfection de salles), sont, au préalable, identifiées et habilitées, par la Direction du Centre informatique national de la MSA, à recevoir un badge d'accès limité aux seules zones d'intervention.

La nuit (19h/7h) et le week-end (24h/24h), l'accès de l'immeuble est interdit sauf aux personnes habilitées sous contrôle de l'agent de surveillance.

Les locaux techniques sont fermés à clé. Les clés des différents locaux sensibles (techniques et autres en permanence verrouillés) ne sont accessibles qu'aux personnes habilitées (par une armoire informatisée de gestion de clés munie d'un lecteur de badge et d'un code).

L'agent de sécurité ne délivre aucune clé, sauf de manière exceptionnelle et à l'aide de son badge et après accord d'un responsable de la sécurité du site (listés dans le cahier de consignes) ; dans ce cas il note la date et l'heure d'entrée et de sortie ainsi que l'identité de ces personnes accédant à ces locaux.

Le Centre Informatique est divisé en cinq zones : les bureaux du personnel, les parties communes, les salles de pilotage des réseaux, les salles des serveurs, les locaux techniques.

1. Les bureaux sont en accès libre.
2. Les parties communes (salles de réunion, restaurant, salles du comité d'entreprise), sont en accès libre.
3. Les salles de pilotage des réseaux ont leurs entrées protégées par un lecteur de badge et réservées au personnel habilité. Elles ne sont pas identifiables de l'extérieur du bâtiment.
4. Les salles des serveurs (baies de disques, salle robots de montage de cartouches, serveurs applicatifs, serveurs de ressources et de gestion des réseaux, zones de tests) relèvent du même niveau de protection que les salles de pilotage réseaux.
5. Les locaux techniques (climatisation, arrivées des lignes télécoms, répartiteurs réseaux et systèmes d'alimentation électrique) sont fermés à clé. Ces clés ne sont accessibles qu'aux personnes habilitées et situées dans une armoire informatisée de gestion de clés, munie d'un lecteur de badge et d'un code.

L'agent de sécurité ne délivre aucune clé, sauf de manière exceptionnelle, à l'aide de son badge et après accord d'un responsable de la sécurité du site (listés dans le cahier de consignes) ; dans ce cas il note la date, le numéro de clé, l'heure d'entrée et de sortie de cette clé ainsi que l'identité des personnes accédant à ces locaux.

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Référentiel Guichet Unique Virtuel

Annexe 10 : *sécurités et secrets (suite)*

Page : 3/9

Sécurité des matériels, protection contre les sinistres naturels :

Le risque de pannes majeures devant être considéré et compte tenu de la situation géographique actuelle du Centre, le Centre informatique national de la MSA dispose de l'ensemble des moyens classiques de prévention présents dans tout site informatique de cette importance :

- régulation et secours de l'alimentation électrique :
 - 2 onduleurs redondants de 200 KVA avec batteries,
 - 1 groupe électrogène d'une puissance de 900 KVA.Ces équipements sont contrôlés et testés mensuellement.
- protection contre l'incendie par système de détection/extinction manuel ou automatique:
 - détecteurs de fumée dans les locaux de types 3, 4 et 5,
 - disjoncteurs automatiques pour l'énergie électrique et climatique,
 - portes et clapets coupe-feu.Ces équipements sont contrôlés et testés mensuellement.
- extinction automatique dans les salles des serveurs par gaz inergène FE13.
- une infrastructure de climatisation nécessaire au bon fonctionnement de certains matériels.

De plus, pour parer aux interruptions des activités de l'entreprise et permettre aux processus cruciaux de continuer malgré des défaillances majeures ou des sinistres impactant le système d'information, le Centre informatique national de la MSA a mis en œuvre et entretient depuis 1982 un **plan de reprise d'activité** avec un prestataire extérieur spécialisé, fournisseur de moyens de secours (backup). Ce plan est mis en œuvre 2 fois par an.

10.2 sécurité des réseaux

Les architectures réseaux sont pourvues d'équipements classiques de type firewalls et proxy serveurs. Une architecture haute disponibilité a été mise en œuvre pour ces plates-formes. Ces matériels, y compris les postes de travail sont dotés d'antivirus mis à jour automatiquement et quotidiennement.

Cette mise à jour peut être manuelle en cas d'attaque par des virus nouveaux et dangereux pour lesquels un antivirus a été mis à disposition très tardivement.

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Référentiel Guichet Unique Virtuel

Annexe 10 : *sécurités et secrets (suite)*

Page : 4/9

De plus, une sensibilisation (consignes) régulière des utilisateurs par messagerie est effectuée.

Echanges de données (Centre informatique national de la MSA/ PARTENAIRE) :

Le produit utilisé pour la télétransmission des données entre le Centre informatique national de la MSA et ses partenaires informatiques est le produit XFB de la société AXWAY, configuré sous les protocoles de transfert de fichiers sécurisés PESIT ou ETEBAC 3, via un réseau de transport TCP/IP en interne et externe et/ou X25 en externe. Les connexions en TCP/IP avec l'extérieur sont, si nécessaire, chiffrées.

Les supports magnétiques (cartouches, CD ROM, DVD ROM) sont transmis exclusivement en envoi recommandé avec accusé de réception.

Un réseau institutionnel privé est utilisé pour les transferts des fichiers entre les centres informatiques régionaux de la MSA (CITI) et le site informatique du Centre informatique national de la MSA.

Pour les échanges internes entre les différentes plates-formes du Centre informatique national de la MSA, le produit XFB est également utilisé au travers d'un réseau privé d'entreprise.

Plusieurs mécanismes sont mis en œuvre pour garantir la sécurité des échanges de fichiers :

- Sur le central, le logiciel de sécurité TSS est utilisé pour contrôler l'accès et l'utilisation de XFB.
- Les accès aux fichiers reçus ou émis par XFB sont contrôlés par TSS. Une normalisation de leurs noms (sens/partenaire/identifiant de fichier /identifiant de transfert) permet de définir le niveau de granularité souhaité pour les habilitations d'accès.
- Les messages relatant les événements de transfert via XFB sont écrits sur un « journal » et permettent de tracer tous les transferts. Sur notre site, ces données sont archivées et pourraient permettre, en cas de litiges, de reconstituer les événements liés à un ou plusieurs transferts.
- Des contrôles sont effectués par XFB avant l'acceptation (connexion entrante) du transfert de fichiers, permettant au niveau des phases de connexions protocolaires la reconnaissance réciproque des partenaires par vérification du nom et du mot de passe.

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Référentiel Guichet Unique Virtuel

Annexe 10 : *sécurités et secrets (suite)*

Page : 5/9

- Pour tous les fichiers émis ou reçus, l'administrateur XFB attribue un identifiant de fichier (IDF) permettant de distinguer les flux applicatifs. Le transfert entre les partenaires est réalisé sur cet identifiant logique, le nom physique du fichier est pris en charge et contrôlé par le récepteur.

- Un exit permet de vérifier l'existence de l'IDF et la cohérence de la longueur des enregistrements des fichiers transférés.

Gestion du réseau de transport :

Réseau Institutionnel :

Le réseau Institutionnel est un réseau de transport privé et sécurisé qui s'appuie sur :

Le Réseau Institutionnel National :

- Le Réseau Institutionnel National s'appuie sur l'offre « Ethernet-Link » de France Télécom. L'interconnexion est effectuée en Ethernet-fibre et un back-bone ATM. Les technologies utilisées limitent considérablement les risques « d'écoute ».
- La vitesse de connexion avec les CITI est de 4 Mbps garantis et 15 Mbps en crête.
- L'interconnexion au Réseau Institutionnel National est réalisée au travers d'un Firewall.
- des matériels actifs de marque Nortel ou Cisco sont utilisés.

Le Réseau Institutionnel Régional :

- Actuellement basés sur l'offre « Transfix » de France Télécom, les Réseaux Institutionnels Régionaux sont progressivement en train de migrer vers l'offre « Ethernet-Link » de ce même opérateur. L'interconnexion est effectuée en Ethernet-fibre et un back-bone ATM. Les technologies utilisées limitent considérablement les risques « d'écoute ».
- L'interconnexion entre le Réseau Institutionnel Régional et le Centre Régional est réalisée au travers d'un Firewall.
- Des matériels actifs de marque Nortel ou Cisco sont utilisés.

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Référentiel Guichet Unique Virtuel

Annexe 10: *sécurités et secrets (suite)*

Page : 6/9

Réseau Parisien :

Le réseau Parisien est un réseau de transport privé et sécurisé qui s'appuie sur :

- Le site de Bagnolet est interconnecté en s'appuyant sur l'offre « Ethernet-Link » de France Télécom. L'interconnexion est effectuée en Ethernet-fibre et un back-bone ATM.
- La vitesse des liaisons entre le Centre informatique national de la MSA et les sites des Mercuriales pour la CCMSA est de 2x10 Mbps garantis et 40 Mbps en crête;
- Des matériels actifs de marque Nortel ou Cisco sont utilisés ;
- Deux frontaux redondants, de marque CISCO, pour l'accès au serveur central.

10.3 sécurité des applications

Seules les personnes des organismes de Mutualité Sociale Agricole sont directement habilités par leur Directeur, à accéder aux informations détaillées à l'annexe 12.

L'Authentification/ Identification de l'utilisateur :

L'accès aux systèmes d'information est strictement réservé aux utilisateurs internes MSA au travers d'un réseau privé d'entreprise. L'accès à chaque serveur et aux applications hébergées, est soumis obligatoirement à un mécanisme d'authentification s'appuyant sur le couple « identifiant/mot de passe ».

Chaque nouvel utilisateur des ressources informatiques du Centre est sensibilisé aux contraintes et obligations inhérentes à la mise en œuvre de la sécurité d'accès. Il lui est attribué un identifiant et accordé les comptes qui sont nécessaires à son travail sur les différents systèmes d'information.

Les mots de passe sont gérés selon une politique d'usage installée sur tous les systèmes. Ses principales caractéristiques sont :

- blocage complet du compte au bout de 3 tentatives de connexions infructueuses
- blocage du compte au bout de 5 semaines après expiration du mot de passe
- un même mot de passe ne peut être réutilisé avant un an et demi
- le changement du mot de passe est obligatoire toutes les 4 semaines
- le mot de passe doit satisfaire à des normes syntaxiques strictes.

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Référentiel Guichet Unique Virtuel

Annexe 10: *sécurités et secrets (suite)*

Page : 7/9

Habilitations :

Les applications mises en œuvre au Centre informatique national de la MSA sont découpées en différentes fonctions (consultation, paramétrage, etc. ...) dès les phases de conception, correspondant à des entités organisationnelles cohérentes. Les ressources informatiques de chacune des fonctions de l'application (programmes, transactions, fichiers, écrans,.. etc.) sont déclarées aux systèmes de sécurité et autorisées en fonction du niveau requis (lecture, écriture, mise à jour, voire interdiction) à des profils d'habilitations. Les combinaisons de profils permettent de définir les habilitations correspondant aux métiers des utilisateurs (liquidateurs, techniciens, informaticiens, ...).

Les responsables d'applications, en relation avec l'administrateur, associent des profils d'habilitations à des groupes d'utilisateurs identifiés. Par plate-forme, un administrateur central de sécurité effectue lui-même le paramétrage de ces habilitations, ou délègue ces tâches aux administrateurs régionaux selon la hiérarchie des contrôles d'habilitation demandée. Cet administrateur central dispose de moyens d'audit et de contrôle pour vérifier la bonne qualité de l'ensemble de ces informations et des « barrières » existent pour se prémunir d'une erreur de manipulation dans l'attribution des profils.

En cas de situation extrême où il est nécessaire de divulguer les mots de passe de niveau système (compte ROOT en UNIX par exemple) et en cas d'absence d'administrateur, un coffre de sécurité fermé à clé est confié à l'agent de gardiennage. Son ouverture n'est autorisée qu'aux personnes figurant sur une liste fermée. Ce coffre, opérationnel pour les serveurs UNIX aujourd'hui, contient les mots de passe de niveau système (ayant donc tous les droits). Ils sont renouvelés et contrôlés tous les mois par la Cellule Sécurité.

La gestion des habilitations est externe aux applications et est pris en charge par l'outil de sécurité seul. Ce logiciel de sécurité en MVS et UNIX fait partie intégrante du système d'exploitation.

Le Centre informatique national de la MSA assure la gestion et coordonne la maintenance du matériel. :

- La maintenance préventive des matériels est planifiée lors d'un après-midi, à chaque fin de mois.
- En cas d'incident grave de fonctionnement touchant les serveurs applicatifs et les unités de stockage disques, une connexion automatique est assurée sur les sites de maintenance matériels des différents constructeurs pour diagnostic et planification des actions de remises en état.

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Référentiel Guichet Unique Virtuel

Annexe 10: *sécurités et secrets (suite)*

Page : 8/9

Confidentialité des données

En fonction de la nature des traitements à réaliser sur les données, il a été nécessaire de les classer et de protéger, plus particulièrement, les données de production. Pour cela, toutes nos architectures techniques sont bâties selon différents environnements de travail afin de cloisonner les différents types de données gérées.

On identifie principalement les environnements de :

- production
- bétatest (ou pré-production)
- simulation
- formation
- développement d'applications.

De plus, de par la nature des données présentes dans le Centre informatique national de la MSA, toutes les procédures de déclarations à la CNIL de fichiers contenant des données personnelles, sont réalisées en relation avec le Département Juridique de la CCMSA.

10.4 sécurité des données

Conformément à l'article 34 de la loi du 6 janvier 1978, les organismes de mutualité sociale agricole s'engagent à prendre toutes les précautions techniques et matérielles nécessaires afin de préserver la sécurité des informations et, notamment, d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

Chaque jour, une sauvegarde complète des données des applications est effectuée après l'arrêt du télétraitement à 18 H. Les cartouches sur lesquelles sont enregistrées les sauvegardes sont transportées le lendemain vers 9h00 et stockées chez un prestataire spécialisé, dans des locaux situés en Seine-Saint-Denis.

Chaque jour, une sauvegarde complète des données et applications gérées par les serveurs de ressources est effectuée à partir de 22h. Un système de sauvegarde centralisées est mis en place et la gestion des cartouches générées est identique à celle du serveur central et des serveurs UNIX.

10.5 secrets

Le personnel de la CCMSA (département de la gestion centralisée) et du Centre informatique national de la MSA est soumis au secret professionnel et ce conformément à l'article 226-13 du Code Pénal.

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Référentiel Guichet Unique Virtuel

Annexe 10: *sécurités et secrets (suite)*

Page : 9/9

II) SECURITE DES CITI

Les sécurités générales relatives au CITI sont celles prévues par le dossier CM/CD contrôle médical - contrôle dentaire.

Un dossier « Contrôle médical - Contrôle dentaire » déposé à la CNIL sous la référence n° 412 037 a reçu un avis favorable de la Commission par délibération n° 96-051 du 04 juin 1996.

10.1 Sécurités physiques

Le serveur sur lequel sont hébergées les données à caractère personnel et les données statistiques, est implanté dans un local sécurisé, dont les accès sont contrôlés.

Pour le contrôle d'accès physique aux locaux où sont accessibles les données à caractère personnel, les dispositifs suivants ont été retenus :
digicode, badge, gardien et alarme

Ce local dispose des sécurités contre l'incendie, d'une alimentation électrique sous onduleur et d'un système de climatisation.

10.2 Sécurités logiques

Sécurités existantes en MSA

Conformément à l'article 34 de la loi du 6 janvier 1978, les organismes de mutualité sociale agricole s'engagent à prendre toutes les précautions techniques et matérielles nécessaires afin de préserver la sécurité des informations et, notamment, d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

Authentification/ Identification de l'utilisateur :

Seules les personnes des organismes de Mutualité Sociale Agricole sont directement habilités par leur Directeur, à accéder aux informations détaillées à l'annexe 12.

L'authentification/ identification de l'utilisateur se fait par mot de passe.

10.3 Secret – Confidentialité

Le personnel des Caisses de MSA et de AGORA est soumis au secret professionnel et ce conformément à l'article 226.13 du Code Pénal.

**DECLARANT**

Numéro de dossier attribué par la CNIL si vous en disposez déjà Dossier n°.....
NOM ou raison sociale **Caisse Centrale de Mutualité Sociale Agricole** Sigle **CCMSA**
N° SIREN ou SIRET **302 990 445** Code APE **753**
Téléphone **01.41.63.77.77**
Adresse électronique

L'ARCHITECTURE INFORMATIQUE, LES SECURITES ET SAUVEGARDES**1. Description du système informatique. Il est constitué :**

- d'un parc de micro-ordinateurs sans serveur central
- d'un mini/petit serveur d'entreprise
- d'un ensemble de serveurs au sein de l'organisme ou externalisés
- d'un gros ordinateur au sein de l'organisme ou externalisé
- par l'hébergement chez un fournisseur internet
- Nom de l'hébergement
- autre architecture informatique :

Nom(s) du (des) fournisseur(s) et du (des) modèle(s) : **IBM, BULL, DELL**.....

Nom(s) du (des) système(s) d'exploitation : **Z/OS, UNIX/AIX, WIN 2000, WIN XP, WIN 2003, LINUX REDHAT**.....

2. Nature du réseau informatique permettant les échanges d'informations en interne.

- aucun réseau (par ex. des micro-ordinateurs isolés)
- un réseau local d'entreprise. Nom (ex. Netware) : **NETWARE**
- un serveur interne accessible de l'extérieur via internet
- un hébergement externe accessible via internet.
- un extranet mis en œuvre par un Réseau Privé Virtuel (RPV ou VPN en anglais).
Nom du dispositif technique ou du prestataire :
- des lignes privatives louées à un opérateur de télécommunication
- utilisation de technologies sans contact. Nom (ex. WiFi) :
- utilisation de postes de travail nomades (ex. micro-ordinateurs) avec VPN SSL et authentification forte
- autre type de réseau :

Nombre total de postes de travail : **1000 à 1500 postes**

Éventuellement, nom(s) du (des) logiciel(s) réseau(x) ou du moniteur de télétraitement :
.....

3. En cas d'échanges d'informations avec des partenaires ou organismes extérieurs, préciser le(s) procédé(s).technique(s) utilisé(s) :

- support magnétique ou analogue (disque, bande, cd-rom, clé USB,..) :
- Chiffrement : **NON**
- messagerie internet. Chiffrement : **NON**
- transfert de fichier par internet. Chiffrement : **NON**
- transfert via un réseau privatif. Nom éventuel du réseau :
- Chiffrement : **NON**
- autre procédé :
- Chiffrement : **NON**

¹ Plusieurs cases peuvent être cochées en réponse à une question

4. Sécurité (protection) physique des locaux et équipements, sauvegarde du système informatique
 Décrire brièvement les dispositifs/procédures permettant d'assurer la sécurité physique des locaux et équipements informatiques (badge d'accès, gardiennage etc.) :

Gardiennage, badges d'accès

- Mesures assurant la sauvegarde du système informatique
 - Type de support utilisé : **Cartouches magnétiques**
 - Fréquence des sauvegardes : **quotidienne**
 - Chiffrement des sauvegardes : **NON**
 - Lieu de stockage : **Seine Saint-Denis**.....
- Protection supplémentaire du lieu de stockage des supports de sauvegarde. Préciser :
Mirroring des données sur UNIX

5. Protection contre les intrusions extérieures utilisant le canal des réseaux informatiques.

Procédé(s) technique(s) utilisé(s) :

- un routeur. Nom :
- un pare-feu (firewall). Nom : **4 Firewall NOKIA CHECKPOINT et 2 PIX CISCO.**
un système complet de détection d'intrusion (IDS). Nom :
- autre procédé : **2 liaisons à 50 Mbps avec équilibrage de charge, antivirus, antispam, reverse proxy, Gateway VPN**.....

6. Mesures destinées à assurer la confidentialité des données lors du développement de l'application informatique.

- Le développement de l'application s'effectue dans un environnement informatique distinct de celui de la production (par ex. sur des ordinateurs différents, dans des salles machine différentes)
- Le personnel affecté aux tâches de développement est distinct de celui assurant la gestion ou l'exploitation des équipements informatiques de production
- La mise au point des logiciels s'effectue sur des données fictives et non sur des données réelles
- Autres mesures destinées à protéger la confidentialité des données de production :
.....

7. Mesures destinées à assurer la confidentialité des données lors des opérations de maintenance des équipements informatiques

- Les interventions de maintenance des matériels sont enregistrées dans une main-courante
- Les interventions de maintenance des matériels par un sous-traitant se font en présence d'un informaticien de l'entreprise
- La télé-maintenance des matériels n'est pas autorisée
- Les supports de stockage envoyés à l'extérieur à fin de réparation font l'objet d'une procédure de protection particulière. Si oui, préciser laquelle : **Dans des valises sécurisées et transport privé banalisé**.....
- Les supports de stockage destinés à la destruction font l'objet d'une procédure de protection particulière. Si oui, faire une description : **Certificat de destruction pour les cartouches**.....

8. Mesures destinées à assurer la confidentialité des données lors des opérations de maintenance des logiciels informatiques

- Les interventions de maintenance des logiciels dans l'environnement de production sont enregistrées dans une main-courante
- Les interventions de maintenance des logiciels de l'environnement de production se font sous le contrôle du chef d'exploitation en respectant une procédure spécifique
- La télé-maintenance des logiciels de l'environnement de production n'est pas autorisée sans contrôle
- Une procédure particulière est mise en œuvre dans le cas où une opération de maintenance logicielle nécessiterait un accès aux fichiers de données nominatives. Si oui, la décrire :

.....
LE LOGICIEL D'APPLICATION

9. Il met en œuvre :

- une base de données.(ou un logiciel de gestion d'un entrepôt de données).Nom :
- un (des) progiciel(s). Nom(s) :
- un infocentre. Nom :
- un logiciel d'analyse de données permettant des statistiques/profilages/segmentations
Nom :
- Autre :

10. Finalités des procédés techniques particuliers

- carte à puce
- biométrie (voir également la rubrique 13)
- RFID (reconnaissance à distance par radio-fréquence)
- vidéo-surveillance
- autre :

11. Authentification/identification des personnes habilitées à accéder à l'application. Le contrôle d'accès se fait-il par :

- un mot de passe.

Préciser :

- s'il a une structure obligatoire (ex. alphanumérique, présence d'un caractère spécial...)
Géré via outils propres à chaque environnement
- sa longueur minimale :
- sa durée de vie avant changement obligatoire :
- s'il y a interdiction de réutiliser les n précédents mots de passe :
- s'il y a interdiction d'utiliser certains mots de passe (ex. date de naissance, prénom,..) :
- s'il y a blocage automatique du terminal d'accès au bout d'un certain nombre d'essais infructueux (si oui, préciser ce nombre) :
- des profils d'habilitation définissant pour chaque utilisateur les fonctions autorisées ou les catégories d'informations accessibles
- une carte à puce
- un dispositif biométrique (voir également la rubrique 13)
- autre
- Lors d'une connexion, des informations concernant la précédente connexion s'affichent sur le terminal (par ex. date, heure et identifiant de l'utilisateur)
- Les accès à l'application font l'objet d'une journalisation (données de connexion). Si oui, préciser les informations journalisées :
 - date/heure de connexion
 - identifiant du poste de travail
 - identifiant de l'utilisateur
 - date/heure de déconnexion
 - autres informations journalisées :
- Les accès aux fichiers de données nominatives de l'application font l'objet d'une journalisation spécifique. Si oui, préciser les informations journalisées :
 - date/heure d'accès
 - identifiant du poste de travail
 - identifiant de l'utilisateur
 - la référence des données du fichier auxquelles il a été accédé
 - autres informations journalisées : **Tentative de violation d'accès**



Commission Nationale de l'Informatique et des Libertés

8 rue Vivienne

CS 30223

75083 Paris Cedex 02

- type d'accès journalisés, pour : CONSULTATION CREATION MISE A JOUR

12. Confidentialité/authentification. L'application met en œuvre des procédés :

- d'anonymisation des données. Nom :
- de chiffrement des données.
Nom (par ex. 3DES) : Gnu PG..... Longueur de la clé : 1024.....
- de chiffrement du transport des données. **OUI**
Nom (par ex. SSL) : Longueur de la clé :
- d'authentification émetteur/ destinataire (signature électronique, certificat,...).
Procédé et nom commercial :
- Expliquer brièvement les raisons du recours à ces procédés :

13. En cas d'usage d'un procédé biométrique. Préciser :

- sa nature (par ex. contour de la main, empreinte digitale, iris,...) :
- le nom commercial du dispositif ou du fournisseur :
- si l'empreinte biométrique est mémorisée sur un support individuel : NON
- si les empreintes biométriques sont mémorisées dans un fichier NON

NB : les traitements de données biométriques sont soumis à autorisation préalable de la CNIL.

A. SENSIBILISATION DES UTILISATEURS A LA POLITIQUE DE SECURITE

- La politique de sécurité/confidentialité est formalisée dans des documents
- Action de sensibilisation des utilisateurs à la politique de sécurité.
Si oui, sous quelle forme (formation, affiche,...) :

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Guichet Unique Virtuel

Annexe 12 : *Catégories d'informations traitées*

Page 1/3

12.1 catégories des données à caractère personnel

A. Les données relatives à l'**identification des personnes** dans les fichiers émis par les systèmes d'information métier au niveau national sont :

- Motifs de gestion Maladie
- Motifs de gestion famille
- Motifs de gestion Invalidité
- Motifs de gestion Vieillesse
- Motifs de gestion Accident du travail et Maladie Professionnelle
- Motifs de gestion cotisation (COTAS et COTNS)
- Motifs de gestion contentieux

Les données « motif de gestion » sont calculées sur la situation des individus en tant que prestataire au sein de la MSA, et sont issues des bases de données métiers régionales. Le motif de gestion caractérise un ensemble ou un sous ensemble de données qui ont été définis afin d'en connaître leurs localisations dans les systèmes d'information respectifs. On peut trouver par exemple comme motif de gestion des données du niveau « domaine » ou « prestation ».

Des traitements au sein de la Caisse Centrale de MSA permettront de contrôler les données envoyées en s'appuyant sur les référentiels d'identification mais également d'alimenter le référentiel Guichet Unique Virtuel.

B. Les données comportent le **Numéro Invariant Large (NIL)**

Ce numéro est un numéro de gestion des individus interne à l'institution de la Mutualité Sociale Agricole sur treize caractères commençant par le chiffre 02 puis du numéro de la caisse, puis d'un numéro de série sur neuf caractères.

C. Le fichier comporte des **données complémentaires** aux motifs de gestion calculés :

- Un code de fin de motif de gestion
- Une date de début d'effet du motif
- Une date de fin d'effet du motif
- Une date de début d'échange de période
- Une date de fin d'échange de période

CAISSE CENTRALE DE LA MUTUALITE SOCIALE AGRICOLE

Guichet Unique Virtuel

Annexe 12 : *Catégories d'informations traitées (suite)*

Page 2/3

12.2 conservation des données à caractère personnel

Les données issues des traitements régionaux envoyées à la CCMSA seront conservées pendant 27 mois dans le référentiel du guichet unique Virtuel avant d'être supprimées. Le référentiel GUV est hébergé au sein du CIMAFAP site de Nanterre.

Le temps de conservation des données au sein du référentiel GUV a été défini en fonction du :

- ✓ Temps de mise à disposition des données de prestation afin de pouvoir répondre aux sollicitations du RNCPS.
- ✓ et du délai de prescription sur les branches métiers famille et maladie qui est de deux ans.

