Ordonnance du DFI

sur les exigences minimales auxquelles doivent satisfaire les mesures techniques et organisationnelles à prendre par les services et institutions utilisant systématiquement le numéro d'assuré AVS en dehors de l'AVS

du …

Le Département fédéral de l'intérieur,

vu l'art. 50*g*, al. 3, de la loi fédérale du 20 décembre 1946 sur l'assurance-vieillesse et survivants[1] (LAVS),
en accord avec le Département fédéral des finances,

arrête:

Section 1 Dispositions générales

Art. 1 Objet

La présente ordonnance vise à garantir que les services et institutions qui utilisent systématiquement le numéro d'assuré prennent les mesures techniques et organisationnelles suffisantes pour:

a. s'assurer que le numéro utilisé est correct;

b. en prévenir toute utilisation abusive.

Art. 2 Champ d'application

[1] La présente ordonnance s'applique à tous les services et institutions qui utilisent systématiquement le numéro d'assuré au sens des art. 50*d* et 50*e* LAVS.

[2] Si l'utilisation systématique porte sur des collections de données dans lesquelles aucune mutation liée au numéro d'assuré n'est effectuée, seules sont applicables les dispositions des art. 6 à 8.

Section 2 Mesures visant à garantir l'utilisation du numéro d'assuré correct

Art. 3 Conception des systèmes informatiques

Les systèmes informatiques sont conçus de manière à exclure toute possibilité d'informations contradictoires concernant le numéro d'assuré valable attribué à une personne donnée.

RS …
1 RS **831.10**

Art. 4 Saisie manuelle du numéro d'assuré

1 Le numéro d'assuré ne peut être saisi manuellement dans une collection de données qu'après vérification de la clé de contrôle suivant la procédure décrite à l'annexe 1.

2 La lecture optique du numéro sous forme de code barre est assimilée à une saisie manuelle.

Art. 5 Sûreté de la source des données saisies

1 Le numéro d'assuré ne peut être saisi dans une collection de données que si la certitude quant à l'exactitude du numéro est suffisante.

2 La certitude quant à l'exactitude du numéro d'assuré est réputée suffisante lorsque ce dernier a été communiqué par une procédure conforme à l'art. 134quater, al. 2 à 4, du règlement du 31 octobre 1947 sur l'assurance-vieillesse et survivants (RAVS[2]).

3 La certitude est suffisante lorsqu'il n'existe aucun doute sur l'identité de la personne correspondant au numéro d'assuré que l'on s'apprête à saisir et que la source du numéro est l'une des suivantes:

a. certificat d'assuré AVS au sens de l'art. 135bis RAVS;

b. carte d'assuré au sens de l'art. 42*a* de la loi fédérale du 18 mars 1994 sur l'assurance-maladie (LAMal[3]) valable au moment de la saisie;

c. communication par écrit ou par voie électronique, d'actualité au moment de la saisie, émanant d'un organe de l'AVS;

d. communication par écrit ou par voie électronique, d'actualité au moment de la saisie, émanant d'un service ou d'une institution recommandés par la Centrale de compensation (CdC) comme étant suffisamment sûrs.

4 La CdC publie sur Internet la liste des services et institutions qu'elle recommande comme étant suffisamment sûrs.

Section 3 Mesures visant à prévenir toute utilisation abusive

Art. 6 Principes

1 L'accès aux collections de données contenant le numéro d'assuré n'est accordé qu'aux personnes qui ont besoin dudit numéro pour remplir leurs tâches. Les droits de lecture et d'écriture dans lesdites collections de données est réservé à ces personnes.

2 RS **831.101**
3 RS **832.10**

2 Lorsque le numéro d'assuré est utilisé systématiquement dans des systèmes complexes, les mesures de protection nécessaires sont prises sur la base d'une analyse détaillée des risques. Cette analyse doit notamment prendre en considération le risque d'un regroupement illicite de collections de données.

3 L'utilisation de ressources informatiques et d'unités de mémoire respecte les normes minimales de sécurité définies dans l'annexe 2.

Art. 7 Transmission de données par les réseaux publics

Lorsque des collections contenant des jeux de données où figure le numéro d'assuré transitent par un réseau public, ils sont cryptés conformément à l'état de l'art.

Art. 8 Utilisation et communication

Les services et institutions qui utilisent le numéro d'assuré veillent à informer leurs collaborateurs, dans le cadre de cours de formation et de perfectionnement, que le numéro d'assuré ne peut être utilisé qu'en rapport avec leurs tâches et ne peut être communiqué que conformément aux prescriptions légales.

Art. 9 Entrée en vigueur

1 La présente ordonnance entre en vigueur le 1er décembre 2007, sous réserve des al. 2 et 3.

2 L'art. 5, al. 3, let. a, entre en vigueur le 1er juillet 2008.

3 L'art. 5, al. 3, let. b, entre en vigueur le 1er janvier 2009.

… Département fédéral de l'intérieur:

Pascal Couchepin

Annexe 1
(art. 4)

Vérification de la clé de contrôle (art. 4)

A. Composition du numéro d'assuré

x_{n-12}	x_{n-11}	x_{n-10}	.	x_{n-9}	x_{n-8}	x_{n-7}	x_{n-6}	.	x_{n-5}	x_{n-4}	x_{n-3}	x_{n-2}	.	x_{n-1}	x_n
Code pays				**Numéro de neuf chiffres**											**Clé de contrôle**
7	**5**	**6**		**1**	**2**	**3**	**4**		**5**	**6**	**7**	**8**		**9**	**7**

B. Logique de la clé de contrôle

La clé de contrôle est le dernier chiffre du numéro (x_n); elle s'obtient par les opérations suivantes:

– multiplier alternativement par 3 et par 1 chaque chiffre, en commençant par l'avant-dernier (x_{n-1}), et additionner ces produits:

  total intermédiaire = $(3x_{n-1}) + (x_{n-2}) + (3x_{n-3})$ …

– déterminer ensuite la valeur (clé de contrôle x_n) qui, ajoutée au total intermédiaire, donnera le prochain multiple de 10.

Remarque:

Si le total intermédiaire est déjà un multiple de 10, la clé de contrôle est 0.

C. Illustration

Numéro d'assuré	**7**	**5**	**6**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**→ ? ←**
Multiplicateur	1	3	1	3	1	3	1	3	1	3	1	3	
Résultat	7	15	6	3	2	9	4	15	6	21	8	27	← total intermédiaire: 123
Valeur à ajouter pour obtenir un multiple de 10	130 est le prochain multiple de 10 après le total intermédiaire 123. La différence, et donc la clé de contrôle, est 7 →												**? = 7**

Annexe 2
(art. 6, al. 3)

Normes minimales de sécurité à respecter pour l'exploitation de ressources informatiques et d'unités de mémoire employeés lors de l'utilisation systématique du numéro d'assuré

1. L'accès aux ressources informatiques et aux unités de mémoire est sécurisé physiquement. En cas d'usage de ressources informatiques et de supports de données mobiles, on veillera par des procédés cryptographiques (codage de données) conformes à l'état de l'art à rendre impossible l'accès et l'utilisation par des personnes non autorisées.
2. L'accès aux ressources informatiques et aux unités de mémoire est protégé par des mesures de sécurité informatique appropriées et correspondant à l'état de l'art et aux risques encourus. Ces mesures comprennent au moins l'emploi de logiciels (antivirus), disponibles dans le commerce et régulièrement mis à jour, de détection et d'élimination des maliciels, et le recours à des systèmes de pare-feu (centraux ou individuels).
3. Les utilisateurs ayant accès aux ressources informatiques et aux unités de mémoire doivent s'authentifier. Si l'authentification se fait au moyen d'un mot de passe, celui-ci est tenu secret et ne peut être communiqué. S'il y a lieu de penser que des personnes non autorisées le connaissent, il est immédiatement remplacé.
4. Les mises à jour d'élimination des erreurs (patches de débogage) sont appliquées aussitôt que possible aux systèmes d'exploitation et aux logiciels.
5. Sur les systèmes informatiques employés, les responsables consignent par écrit les activités et événements importants et les analysent régulièrement.
6. Lorsqu'une ressource informatique ou une unité de mémoire doit être réparée, éliminée ou détruite, il est impératif qu'elle ne contienne plus de numéros d'assuré et que ceux-ci ne puissent pas être reconstitués.