



Ordonnance sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération (OIAM)

Modification du ... Projet du 24 août 2022

Le Conseil fédéral suisse

arrête:

I

L'ordonnance du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaires de la Confédération¹ est modifiée comme suit:

Préambule

vu les art. 26 et 84, al. 1, de la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)²,

vu l'art. 27, al. 5 et 6, de la loi du 24 mars 2000 sur le personnel de la Confédération³,

vu l'art. 186 de la loi fédérale du 3 octobre 2008 sur les systèmes d'information de l'armée⁴,

Art. 2 Champ d'application

La présente ordonnance s'applique aux:

- a. unités de l'administration fédérale centrale au sens de l'art. 7 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA)⁵;

¹ RS 172.010.59

² RS 126

³ RS 172.220.1

⁴ RS 510.91

⁵ RS 172.010.1

- b. unités de l'administration fédérale décentralisée au sens de l'art. 7a OLOGA, dans la mesure où elles ont accès aux moyens informatiques de l'administration fédérale centrale.

Art. 3, al. 1

¹ Un système IAM sert à gérer conjointement des données sur l'identité et les autorisations de personnes, de machines et de systèmes pour les mettre à la disposition des systèmes en aval et d'autres systèmes IAM.

Art. 5 Systèmes IAM

¹ Les organes de la Confédération responsables des systèmes IAM sont:

- a. le secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale (secteur TNI de la ChF), pour tous les systèmes IAM proposés comme services standard et tous les systèmes IAM relevant explicitement du secteur TNI de la ChF;
- b. la Direction des ressources du Département fédéral des affaires étrangères (DFAE), pour le système IAM exploité par l'unité Informatique DFAE;
- c. le secteur TNI de la ChF, pour le système IAM des processus d'assistance, y compris le raccordement au *cloud*;
- d. le Secrétariat général du Département fédéral de la défense, de la protection de la population et des sports (DDPS), pour le système IAM exploité par la Base d'aide au commandement (BAC) du DDPS;
- e. le Secrétariat général du Département fédéral de l'économie, de la formation et de la recherche (DEFR), pour le système IAM exploité par le Centre de services informatiques du DEFR (ISCeco);
- f. l'Office fédéral des routes, pour son système IAM de gestion des équipements d'exploitation et de sécurité des routes nationales.

² Les organes de la Confédération visés à l'al. 1 veillent à ce que la licéité du traitement des données personnelles figurant dans les systèmes IAM dont ils sont responsables soit vérifiée au moins tous les quatre ans par un organe externe.

³ Si la présente ordonnance s'applique aux autorités visées à l'art. 2, al. 1, let. a et c à e, LSI conformément à l'art. 84, al. 3, LSI, celles-ci déterminent elles-mêmes quels organes de la Confédération de leur domaine sont responsables.

⁴ Le service technique compétent demeure responsable du système en aval, et en particulier de l'accès à celui-ci.

Art. 11, al. 2 et 3

² Aucun profilage ne peut être effectué dans ces systèmes.

³ En l'absence d'une base legale particuliere en la matiere, aucune donnee sensible ne peut etre traitee dans ces systemes a l'exception des donnees biometriques visees a l'art. 20, al. 2, LSI.

Art. 13, al. 4

⁴ Les donnees peuvent etre transmises de maniere automatisee a d'autres systemes d'information internes a l'administration federale, dans lesquels elles sont reprises et harmonisees, a condition que le systeme concerne:

- a. dispose d'une base legale prevoyant le traitement des donnees a transmettre et d'un reglement de traitement au sens de l'art. 21 de l'ordonnance du 14 juin 1993 relative a la loi federale sur la protection des donnees (OLPD), et

Art. 14, al. 2

² Les dispositions de l'art. 20, al. 2, LSI relatives a la destruction des donnees biometriques sont reservees.

Titre precedant l'art. 18

Section 6 Mesures de protection des systemes IAM et des services d'annuaires

Art. 18, al. 1 et 2

¹ Les exploitants internes et externes d'elements d'un systeme IAM ou d'un service d'annuaires doivent avoir des instructions ecrites sur la securite de l'information et la gestion des risques. En particulier, chaque organe responsable d'un systeme ou d'un service d'annuaires au sens de la presente ordonnance etablit un reglement de traitement conformement a l'art. 21 OLPD.

² Les systemes IAM et les services d'annuaires qui ne sont pas geres par des organes au sens de l'art. 2 ou sur mandat de ces derniers peuvent etre raccordes a des systemes IAM ou a des services d'annuaires internes a l'administration federale uniquement s'ils respectent les exigences minimales predefinies concernant la securite de l'information.

Art. 20 Systeme global IAM

Les systemes IAM de l'administration federale peuvent etre relies entre eux et aux systemes IAM externes vises a l'art. 21 pour former un systeme global.

Art. 21 Conditions pour le raccordement de systemes IAM externes

Les systemes IAM externes ci-apres peuvent etre raccordes aux systemes IAM de la Confederation afin que les personnes geres dans ces systemes externes puissent acceder aux ressources de celle-ci, pour autant que les conditions et les procedures

énoncées aux art. 22 et 23 soient respectées et que les exploitants s'engagent à respecter la présente ordonnance et les prescriptions qui en découlent:

- a. systèmes IAM des Services du Parlement;
- b. systèmes IAM de l'armée;
- c. systèmes IAM comprenant des collaborateurs cantonaux et communaux au sens de l'art. 9, let. a;
- d. systèmes IAM reconnus par le secteur TNI de la ChF qui sont destinés à la fédération d'identités dans le cadre de la cyberadministration;
- e. fédérations d'identités ou systèmes IAM étrangers dont le raccordement mutuel est prévu dans un traité international, ou
- f. registres des attributs qui mettent à disposition des données relatives à des fonctions professionnelles selon l'annexe, let. b.

II

L'annexe est remplacée par la version ci-jointe.

III

La présente ordonnance entre en vigueur le ... 2023.

...

Au nom du Conseil fédéral suisse:

Le président de la Confédération, ...
Le chancelier de la Confédération, Walter
Thurnherr

Annexe
 (art. 11 et 13, al. 1 et 2)

Catégories de données

Remarque préliminaire: pour la signification des astérisques (), voir l'art. 11, al. 2.*

	Services d'annuaires et systèmes IAM avec des personnes au sens des art. 8 et 9, let. a	Systèmes IAM avec des personnes au sens de l'art. 9, let. b
a. Données relatives à la personne		
1. Nom*	X	X
2. Prénom*	X	X
3. Date de naissance	X	X
4. Sexe	X	X
5. Civilité*	X	X
6. Titre*	X	X
7. Initiales*	X	X
8. Identificateurs personnels locaux	X	X
9. Profession*	X	X
10. Langue de correspondance*	X	X
11. Caractéristiques biométriques personnelles particulières, en particulier scan de l'iris, rétine, scan des veines, empreinte digitale, empreinte palmaire, caractéristiques de la forme du visage et profil de la voix	X	
12. Numéro AVS	X	X
b. Données relatives au rapport avec l'employeur/le mandant		
1. Rapports de travail (interne/externe)*	X	
2. Informations relatives à l'unité d'organisation et aux postes de travail*	X	X
3. Futur rattachement à une unité d'organisation	X	
4. Catégorie de personnel	X	
5. Numéro personnel (y c. cantonal)	X	
6. Fonction*	X	
7. Poste*	X	
8. Identification du système d'information du personnel (source)	X	
9. Date d'entrée et date de départ	X	

	Services d'annuaires et systèmes IAM avec des personnes au sens des art. 8 et 9, let. a	Systèmes IAM avec des personnes au sens de l'art. 9, let. b
10. Numéro de pièce d'identité et/ou de badge	X	X
c. Données de contact		
1. Adresse du lieu de travail et adresse postale professionnelle*	X	X
2. Numéro du bureau*	X	
3. Composantes de l'adresse professionnelle* telles qu'adresse électronique*, numéro de téléphone*, numéro de fax*, adresse VoIP*	X	X
4. Composantes de l'adresse externe* (pour les collaborateurs et les mandataires*) ou de l'adresse privée	X	X
d. Données concernant les fonctions professionnelles		
1. Indications issues des registres professionnels officiels (médecin, personne habilitée à dresser des actes authentiques, avocat, etc.)	X	X
2. Fonction selon le registre du commerce et d'autres registres des représentations	X	X
e. Données techniques		
1. Appareils, raccordements, systèmes, applications, etc.	X	X
2. Composantes de l'adresse, numéros d'identification, etc.	X	
3. Langue du système des appareils, des raccordements, etc.	X	X
4. Clés publiques des certificats numériques*	X	X
5. Groupes d'autorisations	X	X
6. Noms pour la connexion aux systèmes informatiques	X	X
7. Mots de passe	X	X
8. Dernière ouverture de session	X	X
9. Échecs lors d'ouvertures de session	X	X
10. Statut (actif/passif)	X	X
f. Données relatives au contrôle de sécurité relatif aux personnes, si celui-ci a abouti à une déclaration de sécurité sans réserve ou si l'autorité décisionnelle a rendu une décision positive		
1. Degré de contrôle	X	
2. Durée de validité de la déclaration de sécurité	X	