Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la police fedpol

Berne, novembre 2021

Ordonnance sur l'interopérabilité des systèmes d'information Schengen-Dublin

Ordonnance N-IOP

Rapport explicatif relatif à l'ouverture de la procédure de consultation

Table des matières

1. Contexte

Les règlements (UE) 2019/817[1] et (UE) 2019/818[2] portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans les domaines des frontières, de la migration et de la police ont été adoptés le 20 mai 2019 par le Parlement européen et le Conseil de l'Union européenne (UE) et ont été notifiés le 21 mai 2019 à la Suisse en tant que développements de l'acquis de Schengen. En signant l'accord d'association à Schengen (AAS; RS *0.362.31*), la Suisse s'est engagée à reprendre en principe tous les développements de l'acquis de Schengen. Lors de sa session du printemps 2021, l'Assemblée fédérale a adopté l'arrêté fédéral du 19 mars 2021 portant approbation et mise en œuvre des échanges de notes entre la Suisse et l'UE concernant la reprise des règlements (UE) 2019/817 et (UE) 2019/818 (ci-après "règlements IOP de l'UE") relatifs à l'établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (développements de l'acquis de Schengen). Le délai référendaire a expiré le 8 juillet 2021 sans avoir été utilisé. La mise en œuvre des deux règlements IOP de l'UE nécessitent l'adaptation de la loi fédérale sur les étrangers et l'intégration (LEI), de la loi fédérale sur le système d'information commun aux domaines des étrangers et de l'asile (LDEA), de la loi sur la responsabilité (LRCF) et de la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP)[3].

Le présent projet vise à soumettre au Conseil fédéral pour approbation les modifications nécessaires au niveau de l'ordonnance pour la mise en œuvre de l'interopérabilité. D'une part, il s'agit des adaptations de l'ordonnance nécessaires pour la mise en œuvre des modifications de la loi. D'autre part, certaines dispositions des règlements IOP de l'UE nécessitent d'être précisées au niveau de l'ordonnance. En outre, les actes de droit tertiaire (décisions d'exécution) relatifs à l'interopérabilité qui ont été notifiés à la Suisse jusqu'à présent devront être mis en œuvre. À ces fins, une nouvelle ordonnance sur l'interopérabilité des systèmes d'information Schengen-Dublin (ordonnance N-IOP) doit être élaborée. Nombre de dispositions à définir au niveau de l'ordonnance relèvent de la protection des données et visent à préciser les droits d'accès aux systèmes

---

[1] Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) nº 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil, JO L 135 du 22.5.2019, p. 27; modifié en dernier lieu par le règlement (UE) 2021/1152, JO L 249 du 14.7.2021, p. 15

[2] Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816, JO L 135 du 22.5.2019, p. 85; modifié en dernier lieu par le règlement (UE) 2021/1150, JO L 249 du 14.07.2021, p. 1

[3] Arrêté fédéral du 19 mars 2021 portant approbation et mise en œuvre des échanges de notes entre la Suisse et l'UE concernant la reprise des règlements (UE) 2019/817 et (UE) 2019/818 (ci-après "règlements IOP de l'UE") relatifs à l'établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE (développements de l'acquis de Schengen), FF 2021 674

d'information Schengen-Dublin ainsi que la conservation, l'archivage et la destruction des données.

1.1. Interopérabilité: généralités

Avec l'interopérabilité, quatre composants centraux seront notamment mis en place. Est ainsi élaboré le portail de recherche européen (ESP) qui permet de consulter simultanément tous les systèmes d'information de l'UE concernés (système d'information Schengen [SIS], système d'identification des empreintes digitales permettant de comparer les données relatives aux empreintes digitales de tous les demandeurs d'asile ainsi que de certains ressortissants d'États tiers et d'apatrides [Eurodac], système d'information sur les visas [VIS], système d'entrée et de sortie [EES], système européen d'information et d'autorisation concernant les voyages [ETIAS] et système européen d'information sur les casiers judiciaires de ressortissants d'États tiers [ECRIS-TCN; il ne s'agit pas d'un développement de Schengen ou de Dublin]) ainsi que les bases de données d'Europol et d'Interpol. L'interopérabilité prévoit en outre l'enregistrement centralisé des données d'identité biométriques et alphanumériques dans le répertoire commun de données d'identité (CIR), et le service partagé d'établissement de correspondance biométriques (sBMS). Elle permettra également de détecter efficacement des identités multiples grâce au détecteur d'identités multiple (MID). L'interopérabilité ne vise pas à collecter de nouvelles données, mais à créer de nouvelles fonctions pour les systèmes d'information actuels (SIS, VIS, Eurodac) et futurs (EES, ETIAS, ECRIS-TCN). Dans les règlements de l'UE, il est question de l'interopérabilité des "systèmes d'information de l'UE". S'agissant de la transposition juridique en Suisse, on se référera en revanche à l'interopérabilité des "systèmes d'information Schengen-Dublin", car seule cette dernière devra être inscrite dans le droit suisse. Selon le calendrier actuel de la Commission européenne, le sBMS devra être mis en service en mai 2022, le CIR d'ici à l'été 2022, et l'ESP ainsi que le MID probablement d'ici à l'été ou à la fin 2023. Actuellement, l'UE prévoit la mise en service de l'interopérabilité à la fin 2023 ou au début 2024. La date précise sera fixée ultérieurement par la Commission européenne. Afin de garantir que la Suisse soit prête sur le plan technique lorsque l'UE rendra opérationnelle l'interopérabilité, il est prévu de mettre en vigueur l'ordonnance N-IOP à la fin 2022.

1.2. Modifications de l'ordonnance nécessaires

Afin de permettre l'interopérabilité des systèmes d'information Schengen-Dublin, les quatre composants centraux à mettre nouvellement en place devront être reliés aux systèmes d'information et aux banques de données de police, qui sont respectivement réglementés dans la LEI et dans la LSIP. Par souci de transparence, les dispositions relatives aux composants centraux sont fixées dans ces deux lois.

L'ordonnance N-IOP vise notamment à mettre en œuvre les quatre nouveaux composants centraux. Des modifications ponctuelles doivent en outre être apportées à d'autres ordonnances qui règlementent les systèmes d'information Schengen-Dublin concernés par l'interopérabilité. Cependant, ces modifications ne font pas l'objet du présent projet et seront soumises au Conseil fédéral en temps voulu.

2. Ordonnance N-IOP

L'ordonnance N-IOP est divisée en huit sections: Objet et définitions (section 1: art. 1 et 2), Service partagé d'établissement de correspondances biométriques (section 2: art. 3 à 7), Répertoire commun de données d'identité (section 3: art. 8 à 17), Portail de recherche européen (section 4: art. 18 à 20), Détecteur d'identités multiples (section 5: art. 21 à 28), Droits des personnes concernées (section 6: art. 29 et 30), Sécurité des données (section 7: art. 31) et Dispositions finales (section 8: art. 32).

Section 1

La section 1 offre un aperçu de la teneur des dispositions visant à mettre en œuvre l'interopérabilité des systèmes d'information Schengen-Dublin en vertu des art. 110 à 110*i* et 120*d* LEI, 16*a* à 16*f* LSIP et des règlements IOP de l'UE.

Art. 1

Cet article présente l'objet de l'ordonnance N-IOP. Celle-ci règle les droits de consultation concernant l'ESP et le MID (let. a), la mise à jour du sBMS (let. b), le droit à consulter le CIR (let. c), la procédure de vérification manuelle des différentes identités dans le MID (let. d), la responsabilité du traitement des données dans le MID, le CIR et le sBMS (let. e), les droits des personnes concernées (let. f), ainsi que la protection des données et la sécurité des données (let. g).

Art. 2

Cet article présente les termes utilisés dans l'ordonnance. Il attribue différentes couleurs aux liens pouvant être établis dans le MID dans le cadre d'une vérification des différentes identités ainsi qu'après une vérification par l'autorité compétente, à savoir jaune (let. a), vert (let. b), rouge (let. c) et blanc (let. d), et renvoie pour leur définition aux dispositions pertinentes des règlements IOP de l'UE (art. 30 à 33) qui règlent en détail ces différents liens. S'agissant de la définition d'"infractions terroristes" et d'"infractions graves", les règlements IOP de l'UE et les bases légales de l'UE relatives au SIS renvoient à la directive (UE) 2017/541[4] et à la décision-cadre

[4] Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, JO L 88 du 31.3.2017, p. 6

2002/584/JAI[5]. Ces termes, qui sont utilisés à l'art. 12 de l'ordonnance, sont précisés dans les annexes 1*a* et 1*b* de l'ordonnance N-SIS (RS *362.0*). Il y a donc lieu de faire référence dans cette ordonnance aux annexes 1*a* et 1*b* de l'ordonnance N-SIS (let. e et f). Les listes des infractions ont été inscrites dans la loi dans le cadre du projet "Prüm Plus"[6]. Il convient donc d'adapter en conséquence la référence dans la présente ordonnance.

Section 2

La section 2 comprend des dispositions sur le sBMS. Ce dernier devra permettre de comparer des données biométriques issues de tous les systèmes d'information Schengen-Dublin. Le sBMS stocke les modèles biométriques qu'il génère à partir des données biométriques de l'EES, du système central d'information sur les visas (C-VIS) et du SIS, et qu'il générera à l'avenir à partir de celles d'Eurodac. Il ne constitue pas un "fichier", c'est-à-dire un ensemble de données, au sens de l'art. 3, let. g, de la loi fédérale sur la protection des données (LPD, RS *235.1*), étant donné que les modèles biométriques (en anglais *templates*) ne permettent pas de remonter aux personnes concernées. Bien que les autorités ont un accès direct au SIS et au CIR, elles ne l'ont pas au sBMS. Étant donné que ce dernier, contrairement au CIR, est également relié au SIS, son contenu est régi non seulement par la LEI (art. 110), mais également par la LSIP (art. 16*a*). Même si les dispositions relatives au sBMS des règlements IOP de l'UE sont directement applicables, ce système a également été réglé formellement dans la loi par souci d'exhaustivité et afin de pouvoir s'y référer plus aisément.

Art. 3

Cet article prévoit que le Secrétariat d'État aux migrations (SEM) et fedpol ont responsables du traitement des données dans le sBMS. La base légale est l'art. 40, par. 1, des règlements IOP de l'UE, qui attribue la responsabilité en matière de traitement des données dans le sBMS aux autorités des États membres chargées du traitement dans l'EES, le VIS et le SIS. Alors que le SEM est responsable des données provenant de l'EES et du C-VIS, la responsabilité de celles issues du N-SIS revient à fedpol.

Art. 4

L'*al. 1* a pour objet les modèles biométriques du sBMS. Ce système stocke les modèles biométriques générés à partir des empreintes digitales et des images faciales. La base légale à cet

[5] Décision-cadre du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres, JO L 190 du 18.7.2002, p. 1; modifié en dernier lieu par la décision-cadre 2009/299/JAI, JO L 81 du 27.3.2009, p. 24

[6] Prüm Plus comprend les accords suivants: l'accord sur la coopération transfrontalière (coopération de Prüm), le Protocole Eurodac entre la Suisse et l'UE et l'accord avec les États-Unis.

égard est l'art. 13, par. 1, des règlements IOP de l'UE, qui règle le stockage des modèles biométriques dans le sBMS. Cet article renvoie à son tour aux bases légales de l'UE relatives au SIS (données visées à l'art. 20, par. 2, pt. w et x, à l'exception des données relatives aux empreintes palmaires du règlement [UE] 2018/1862[7], et les données visées à l'art. 4, par. 1, pt. u et v, du règlement [UE] 2018/1860[8]), à l'EES (données visées aux art. 16, par. 1, pt d, 17, par. 1, pt. b et c, et 18, par. 2, pt. a, b et c, du règlement [UE] 2017/2226[9]) et au VIS (données visées à l'art. 9, nº 6, du règlement [CE] nº 767/2008[10]). Il n'est pas nécessaire de mentionner les photographies dans le texte de l'ordonnance. L'art. 13 des règlements IOP de l'UE renvoie en effet aux dispositions relatives aux différents systèmes dont les données servent à générer les modèles destinés au sBMS. À l'art. 20, par. 2, pt w, des règlements (UE) 2018/1862 (SIS Police) et (UE) 2018/1861 (SIS Frontières), les photographies sont indiquées en plus des images faciales. Toutefois, comme il faudra encore plusieurs années à l'UE avant que les photographies soient stockées dans le sBMS, elles n'ont pas besoin de figurer actuellement dans l'ordonnance N-IOP.

L'*al. 2* prévoit que les modèles biométriques soient enregistrés dans le sBMS séparément les uns des autres et de façon logique selon le système d'information dont ils proviennent. Cette exigence découle de l'art. 13, par. 1, des règlements IOP de l'UE.

Art. 5

Selon l'*al. 1*, si de nouveaux ensembles de données sont saisis ou mis à jour dans l'EES, le C-VIS, Eurodac ou le SIS, le sBMS procède toujours à une comparaison automatisée de ces données avec les données biométriques enregistrées dans le CIR et le SIS. C'est sur la base de ces dernières que le sBMS génèrera des modèles. Les données concernées du CIR proviennent du SIS, de l'EES, du VIS et d'Eurodac (l'ETIAS fait exception, car aucune donnée biométrique n'y est enregistrée). Des règles détaillées relatives au sBMS figurent au chap. III des deux règlements IOP de l'UE. Les modèles biométriques sont introduits dans le sBMS uniquement après que ce dernier a effectué un contrôle automatisé de la qualité des données biométriques ajoutées

---

[7] Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) nº 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission, JO L 312 du 7.12.2018, p. 56; modifié en dernier lieu par le règlement (UE) 2021/1150, JO L 249 du 14.7.2021, p. 1

[8] Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier, JO L 312 du 7.12.2018, p. 1; modifié en dernier lieu par le règlement (UE) 2021/1152, JO L 249 du 14.7.2021, p. 15

[9] Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) nº 767/2008 et (UE) nº 1077/2011, JO L 327 du 9.12.2017, p. 20; modifié en dernier lieu par le règlement (EU) 2021/1152, JO L 249 du 14.7.2021, p. 15

[10] Règlement (CE) nº 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS), JO L 218 du 13.8.2008, p. 60; modifié en dernier lieu par le règlement (EU) 2021/1152, JO L 249 du 14.7.2021, p. 15

à l'un des systèmes d'information Schengen-Dublin, pour s'assurer du respect d'une norme minimale en matière de qualité des données. Cette exigence découle de l'art. 13, par. 3, des deux règlements IOP de l'UE. Conformément à l'annexe de la décision d'exécution[11] relative à l'art. 13, par. 5, des deux règlements IOP de l'UE, on procède soit à une comparaison "un à un" soit à une comparaison "un à plusieurs". Alors que la première consiste en un processus de vérification comparant deux séries de données biométriques, la seconde compare le modèle extrait des données d'entrée biométriques avec les modèles stockés dans la base de données du sBMS.

L'*al. 2* établit que les recherches à l'aide de données biométriques doivent être menées conformément aux finalités prévues à l'art. 14 des deux règlements IOP de l'UE. À cet égard, cet article renvoie à son tour aux bases légales s'appliquant au SIS, à l'EES et au VIS, à savoir aux règlements (CE) nº 767/2008, (UE) 2017/2226, (UE) 2018/1860, (UE) 2018/1861, (UE) 2018/1862 et (UE) 2019/816, sans préciser davantage ces références.

Art. 6

Cet article établit que la durée de conservation dans le sBMS des modèles biométriques et des références aux systèmes d'information de l'UE dont ils sont issus est la même que celle des données biométriques stockées dans le SIS ou le CIR. Le sBMS stocke les modèles biométriques qu'il génère à partir des données biométriques du SIS, de l'EES, du C-VIS et d'Eurodac. Le CIR fait partie de ces trois derniers systèmes. En outre, chaque modèle contient une référence au système d'information de l'UE dont il provient, ainsi qu'une référence aux ensembles de données qu'il contient. L'effacement des données biométriques dans le SIS ou le CIR entraîne automatiquement l'effacement des données dans le sBMS. Cette disposition vise à mettre en œuvre l'art. 15 des règlements IOP de l'UE.

Art. 7

Cet article règle la tenue de registres. Il précise que chaque consultation des modèles biométriques dans le sBMS doit être consignée dans un registre. La Confédération doit tenir les registres, l'autorité responsable étant celle qui consulte le système d'information Schengen-Dublin sous-jacent. L'obligation de tenir des registres qui incombe aux États Schengen-Dublin découle de l'art. 16, par. 2, des règlements IOP de l'UE. Le présent art. 7 fixe les informations à consigner: l'autorité qui consulte le système (let. a), les systèmes d'information Schengen-Dublin consultés (let. b), la date et l'heure de la recherche (let. c), les données biométriques utilisées pour effectuer la recherche (let. d), les résultats de la recherche (let. e). Consigner ces informations dans un

[11] Annexe de la décision d'exécution de la Commission du 26 août 2021 établissant les exigences relatives aux performances du service partagé d'établissement de correspondances biométriques et les modalités pratiques pour le suivi desdites performances en application de l'article 13, paragraphe 5, du règlement (UE) 2019/817 du Parlement européen et du Conseil, C(2021) 6159 final

registre vise à garantir que les droits concédés aux personnes concernées à la section 6 de l'ordonnance seront effectivement respectés. Les données biométriques au sens de la let. d sont les données utilisées pour effectuer la recherche (par ex. des empreintes digitales). Les résultats de la recherche au sens de la let. e contiennent les modèles biométriques.

Section 3

Cette section comprend des dispositions sur le CIR. Un dossier individuel est créé dans le CIR pour chaque personne enregistrée dans l'EES, le C-VIS, ETIAS ou Eurodac, comprenant – si disponibles – ses données d'identité, ses données de documents de voyage et ses données biométriques issues des systèmes d'information Schengen-Dublin précités. Le CIR remplace une partie du système central des différents systèmes d'information Schengen-Dublin (C-VIS, Eurodac, EES et ETIAS), dans la mesure où certaines données alphanumériques (données d'identité et données de documents de voyage) et biométriques de ces systèmes d'information sont stockées dans le CIR. Il constitue ainsi une partie de ces systèmes. Les données du SIS ne sont pas stockées dans le CIR, car l'architecture du SIS est trop complexe à cet effet. Le CIR est notamment destiné à faciliter l'identification correcte de personnes enregistrées dans l'un des systèmes d'information susmentionnés et à aider à cette identification conformément à l'art. 20 des règlements IOP de l'UE (art. 17, par. 1). La LEI constitue la base légale nationale du CIR. Elle précise quelles données restent stockées dans le système central de chacun des systèmes d'information concernés et lesquelles sont désormais stockées dans la partie du CIR. Les dispositions pertinentes se trouvent aux art. 110*a* à 110*d* LEI.

Art. 8

Cet article établit que le SEM est responsable du traitement des données dans le CIR. En vertu de l'art. 40, par. 2, des règlements IOP de l'UE, la responsabilité du traitement des données dans le CIR revient à l'autorité de l'État membre responsable du traitement dans l'EES, le VIS et ETIAS. Par conséquent, c'est le SEM qui assume cette responsabilité en Suisse.

Art. 9

L'*al. 1* fixe que les données d'identité, les données de documents de voyage et les données biométriques de ressortissants d'États tiers sont enregistrées dans le CIR séparément les unes des autres et de façon logique selon le système d'information dont elles sont issues, conformément à l'art. 18, par. 1, des règlements IOP de l'UE.

Il est expliqué à l'*al. 2* qu'une adaptation des données de documents de voyage et des données biométriques de ressortissants d'États tiers dans l'EES, ETIAS, le C-VIS ou Eurodac entraîne automatiquement une adaptation correspondante des données contenues dans le CIR. Cette précision découle de l'art. 19 des règlements IOP de l'UE qui règle l'ajout, la modification et la

suppression de données dans le CIR. Lorsqu'un lien blanc ou rouge est établi dans le MID entre des données issues des systèmes d'information dont le CIR constitue une partie, il s'agit d'un cas particulier. Alors, au lieu de créer un nouveau dossier individuel, le CIR ajoute les nouvelles données au dossier individuel des données liées (art. 19, par. 2, des règlements IOP de l'UE).

L'*al. 3* renvoie à l'annexe 1 de l'ordonnance où figure un catalogue de données reposant sur l'art. 18 des règlements IOP de l'UE et énumérant les données que le CIR contiendra. Étant donné que ce dernier est un système d'information, il faut dresser un catalogue de données, y compris une matrice des droits de consultation. Les données qui seront enregistrées dans le CIR conformément à l'art. 18 des deux règlements IOP de l'UE peuvent relever de trois catégories: données personnelles, données de documents de voyage et données biométriques. Les art. 10, 11 et 12 de l'ordonnance établissent dans quelle mesure les autorités peuvent consulter ces données. Les droits de consultation figurent également à l'annexe 1.

Art. 10

À l'*al. 1* sont énumérées les unités organisationnelles de la Confédération qui peuvent consulter les données enregistrées dans le CIR afin d'identifier des personnes conformément à l'art. 110*b* LEI. L'accès au CIR à des fins d'identification est accordé à des autorités assumant des tâches de police, à savoir fedpol, les autorités de police des cantons et des communes ainsi que l'AFD ou l'Office fédéral de la douane et de la sécurité des frontières (OFDF; désignation officielle dès le 1er janvier 2022) dans le cadre de ses tâches douanières et non douanières, afin de protéger la population et de sauvegarder la sécurité intérieure (art. 110*b*, al. 3, LEI). Ces autorités doivent être indiquées de manière plus précise dans l'ordonnance (dans la mesure du possible, c'est la tâche spécifique et non la désignation actuelle de l'autorité qui est inscrite, comme c'est le cas dans d'autres projets d'ordonnance pour garantir la sécurité juridique). Les services de fedpol ci-après pourront consulter le CIR à des fins d'identification (let. a): la Police judiciaire fédérale (PJF) (ch. 1), le Service fédéral de sécurité (ch. 2), la Centrale d'alarme et d'engagement (EAZ fedpol; ch. 3), les services chargés du traitement des données signalétiques biométriques (ch. 4) et le service chargé de l'échange international d'informations de police relatives aux manifestations sportives, s'agissant de la collecte et de l'échange d'informations en vue d'écarter les dangers pour la sécurité publique ou de maintenir la sûreté intérieure ou extérieure (ch. 5). Tous ces services étant chargés d'effectuer des contrôles des personnes, l'identification de ces dernières constitue une part essentielle de leurs tâches. À l'OFDF, ce sont les collaborateurs chargés du contrôle des personnes qui pourront consulter le CIR à des fins d'identification (let. b). Cette formulation s'inspire de celle de l'art. 4 de l'ordonnance sur le système d'entrée et de sortie (OEES; pas encore en vigueur). Les identifications doivent contribuer à la prévention de l'immigration illégale et à la lutte contre celle-ci ainsi qu'à l'établissement d'un niveau élevé de sécurité (art. 2,

par. 1, let. b et c, des règlements IOP de l'UE), mais il revient aux États Schengen-Dublin de fixer les finalités précises de l'identification (art. 20, par. 5, des règlements IOP de l'UE). Il faudra éviter toute discrimination à l'encontre de ressortissants d'États tiers, fixer les finalités précises de l'identification, énumérer les autorités habilitées à consulter le CIR et définir les procédures, les conditions et les critères de ces contrôles. L'art. 110*b* LEI répond à ces exigences préalables; des contraintes supplémentaires ne semblent pas nécessaires. En outre, toutes les unités organisationnelles mentionnées à l'art. 10, let. a et b, effectueront des tâches permettant de poursuivre les finalités prévues à l'art. 2, par. 1, let. b et c, des règlements IOP de l'UE.

Les unités organisationnelles de la Confédération faisant l'objet de l'al. 1, l'*al. 2* règle l'accès au CIR des autorités de police des cantons et des communes. Selon cet alinéa, les autorités de police cantonales et communales peuvent également consulter les données enregistrées dans le CIR à des fins d'identification. Cette disposition repose sur l'art. 110*b*, al. 3, let. b, LEI qui accorde ce droit à ces autorités de police.

L'*al. 3* règle la procédure de consultation du CIR à des fins d'identification. La consultation se fait à l'aide des données biométriques recueillies directement sur place lors d'un contrôle d'identité. La personne concernée doit être présente au moment où la procédure est lancée. Si les données biométriques de la personne concernée ne peuvent pas être utilisées ou que la recherche à l'aide de ces données échoue, la consultation est réalisée à l'aide de données d'identité de cette personne, combinées aux données de documents de voyage, ou de données d'identité fournies par cette personne. Toute discrimination à l'encontre de ressortissants d'États tiers est à éviter. Cette disposition repose sur l'art. 20, par. 2 et 3, des règlements IOP de l'UE. Lorsque la consultation du CIR à des fins d'identification génère une concordance indiquant que des données sur la personne concernée y sont enregistrées, l'autorité autorisée obtient, conformément aux al. 1 et 2, les données mentionnées à l'annexe 1 de l'ordonnance qui sont stockées dans le système (cf. art. 9, al. 3). L'unité organisationnelle concernée ne peut toutefois pas savoir de quel système d'information sous-jacent au CIR sont issues les données.

L'*al. 4* précise qu'en cas de catastrophe naturelle, d'accident ou d'actes de violence, les autorités autorisées visées à l'al. 1 ne peuvent consulter le CIR que pour identifier, au moyen de données biométriques de l'intéressé, une personne inconnue qui ne peut décliner son identité ou des restes humains non identifiables par un autre moyen. Il revient aux États membres de définir ce qu'ils entendent par "catastrophe naturelle", "accident" ou "actes de violence", dans la mesure où des raisons objectives le justifient. Il s'agit par exemple d'un glissement de terrain ou d'une avalanche (catastrophe naturelle), du crash d'un avion ou d'un accident de la route (accident) ou d'un assassinat (acte de violence). À cet égard, les bases légales se trouvent à l'art. 20, par. 4, des règlements IOP de l'UE.

Art. 11

Cet article énumère les unités organisationnelles de la Confédération et des cantons habilitées, en vertu de l'art. 110c LEI, à consulter les données et les références enregistrées dans le CIR en vue de détecter les identités multiples. S'il existe un lien jaune dans le MID, la consultation est effectuée à des fins de vérification et, s'il existe un lien rouge, à des fins de lutte contre l'usurpation d'identité. Les unités organisationnelles obtiennent ensuite l'accès aussi bien aux données stockées dans le CIR qu'aux références indiquant le système d'information dont ces données sont issues. Bien qu'il s'agisse pour l'essentiel d'une répétition des dispositions de l'art. 110*c*, al. 1, LEI, il convient de les reproduire ici par souci de clarté et d'exhaustivité, étant donné que tous les droits d'accès au CIR doivent être réglementés dans l'ordonnance. Dans la mesure du possible, les unités organisationnelles mentionnées dans le texte de loi sont précisées (let. a, b, ch. 1, et c, ch. 1, 2 et 3). En outre, le bureau SIRENE doit pouvoir, conformément à la let. a, inclure dans la vérification biométrique des données d'identité les services de fedpol chargés du traitement des données signalétiques biométriques. La Section Identification et consultation des visas (SnCV) du SEM, qui détient la souveraineté des données s'agissant de ces informations, doit par ailleurs être en mesure d'aider à la mise à jour des signalements dans le SIS qui relèvent du domaine migratoire. Le bureau SIRENE est cependant toujours responsable en dernier ressort dans ces cas. C'est ce que l'art. 11, let. a, vise à préciser. Les unités du Domaine de direction Immigration et intégration du SEM chargées de l'octroi des visas, conformément à la let. c, al. 1, comprendront également le service central d'expertise MID (*zentrale MID-Expertenstelle*), qui sera créé afin de soutenir la vérification manuelle des liens dans le MID et pourra consulter les données et les références enregistrées dans le CIR. Ce service central d'expertise MID sera composé de membres du personnel des offices fédéraux. Il fournira un soutien sur le plan technique et du personnel aux autorités chargées de la vérification manuelle dans des cas particulièrement complexes ou lorsqu'une autorité ne disposera pas de l'expertise nécessaire à la vérification d'un lien dans le MID.

Art. 12

Cet article énumère les unités organisationnelles de la Confédération habilitées, en vertu de l'art. 110*d* LEI, à consulter le CIR en vue de prévenir et de détecter les infractions terroristes ou d'autres infractions pénales graves, ou d'investiguer en la matière. Concrètement, les autorités mentionnées peuvent consulter le CIR pour vérifier si des données sur une personne précise y sont enregistrées. Il faut à cette fin qu'il existe, dans un cas donné, des motifs raisonnables laissant penser que la consultation servira à la prévention ou à la détection d'infractions terroristes ou d'autres infractions pénales graves, ou aux investigations en la matière. Si, en réponse à une recherche, le CIR indique que des données sur la personne concernée sont enregistrées dans un système d'information Schengen-Dublin, il fournit aux autorités une référence vers le système

correspondant. S'agissant de la définition d'une infraction terroriste ou d'une infraction pénale grave, on se référera à l'art. 2, let. e et f, de l'ordonnance. fedpol, le Service de renseignement de la Confédération (SRC), le Ministère public de la Confédération (MPC), les autorités cantonales de police et de poursuite pénale et les autorités de police des villes de Zurich, Winterthour, Lausanne, Chiasso et Lugano (art. 110*d*, alt. 2, LEI) peuvent consulter le CIR en vue de prévenir ou de détecter les infractions terroristes ou d'autres infractions pénales graves, ou d'investiguer en la matière. Il s'agit ici d'autorités assumant des tâches dans ces domaines. Alors que l'al. 1 traite des droits d'accès des unités organisationnelles de la Confédération, l'al. 2 règle l'accès des autorités cantonales de police et de poursuite pénale et des autorités de police des villes de Zurich, Winterthour, Lausanne, Chiasso et Lugano. Les services ci-après de fedpol peuvent consulter le CIR dans le but de prévenir ou de détecter les infractions terroristes ou d'autres infractions pénales graves, ou d'investiguer en la matière (let. a): la PJF (ch. 1), les services chargés du traitement des données signalétiques biométriques (ch. 2) et l'EAZ fedpol (ch. 3). Au sein du SRC, les services ci-après disposent également d'un droit de consultation (let. b): la division Acquisition (ch. 1), la division Analyse (ch. 2), la coordination Lutte contre le terrorisme (ch. 3), la coordination Service de renseignement prohibé (ch. 4), la coordination Lutte contre l'extrémisme (ch. 5), la coordination Non-prolifération (ch. 6), le domaine Service des étrangers (ch. 7), le domaine Saisie des données/Triage (ch. 8) et le Centre fédéral de situation (ch. 9). Cette liste repose sur l'art. 12 de l'OEES, qui est actuellement au stade de projet et n'est pas encore en vigueur. Le SRC a demandé d'inclure en outre le domaine Saisie des données/Triage et le Centre fédéral de situation, qui mènent des activités dans le domaine de la prévention et de la détection des infractions terroristes ou d'autres infractions pénales graves, ou des investigations en la matière. Enfin, au MPC, les divisions conduisant les procédures pourront consulter le CIR en vue de prévenir ou de détecter les infractions terroristes ou d'autres infractions pénales graves, ou d'investiguer en la matière (let. c). Celles-ci sont définies à l'art. 1, al. 2, du règlement du 26 février 2021 sur l'organisation et l'administration du Ministère public de la Confédération (RS *173.712.22*).

L'*al. 2* vise à habiliter les autorités cantonales de police et de poursuite pénale ainsi que les autorités de police des villes de Zurich, Winterthour, Lausanne, Chiasso et Lugano à consulter les références enregistrées dans le CIR aux fins prévues à l'al. 1. La base légale leur accordant cette possibilité se trouve à l'art. 110*d*, al. 2, let. d, LEI.

Art. 13

L'*al. 1* règle la première des deux étapes de la procédure prévue à l'art. 22 des règlements IOP de l'UE. Si cette première étape aboutit à une réponse positive (autrement dit, si des données sur une personne sont disponibles dans l'EES, ETIAS, le C-VIS ou Eurodac), le CIR indique à

l'autorité qui a effectué la recherche quel système d'information contient des données. Cette information ne peut être utilisée qu'aux fins de transmission de la demande d'accès complet prévue à l'al. 2. La base légale à cet égard se trouve à l'art. 110*d*, al. 3, LEI.

L'*al. 2* règle la seconde étape de la procédure (art. 22 des règlements IOP de l'UE). En cas de réponse positive au sens de l'al. 1, l'autorité qui a procédé à la recherche soumet à l'EAZ fedpol une demande d'accès complet à au moins l'un des systèmes d'information ayant fourni une réponse positive. L'accès complet reste soumis aux conditions et procédures fixées dans les instruments juridiques pertinents. La base légale concernée se trouve à l'art.110*d*, al. 4, LEI. La demande doit exposer les conditions de l'accès complet au système concerné, prévues par les bases légales correspondantes. Il s'agit d'éviter ainsi tout hameçonnage, c'est-à-dire qu'une consultation soit effectuée sans que des motifs raisonnables laissent penser qu'une personne soit répertoriée dans les systèmes. D'une manière très générale, cela vise à prévenir les abus. Des motifs raisonnables doivent exister pour accéder aux données du CIR à des fins de poursuite pénale.

L'*al. 3* décrit la procédure à suivre lorsqu'exceptionnellement aucune demande d'accès complet au sens de l'al. 2 n'est déposée. Dans ce cas, l'autorité qui a effectué la recherche conformément à l'al. 2 et à l'art. 22, par. 2, des règlements IOP de l'UE est tenue de consigner les motifs de cette renonciation dans un fichier national traçable. Il s'agit également de prévenir ainsi l'hameçonnage et les abus. La surveillance indépendante du traitement des données est réglée à l'art. 30 de l'ordonnance, lequel permet de respecter effectivement les droits concédés aux personnes concernées à la section 6.

Art. 14

L'*al. 1* contraint l'EAZ fedpol, avant qu'elle approuve une demande d'accès complet aux données conformément à l'art. 12, al. 2, de l'ordonnance, de s'assurer que les données peuvent contribuer à prévenir ou à détecter des infractions terroristes ou d'autres infractions pénales graves, ou à investiguer en la matière (let. a) et qu'il existe des preuves ou des motifs suffisants permettant de considérer que la communication des données contribuera à atteindre le but visé (let. b). Cette énumération vise à mettre en œuvre l'art. 22, par. 1, des règlements IOP de l'UE, qui ne permet la consultation du CIR que s'"il existe des motifs raisonnables de croire que [cela] contribuera à la prévention ou à la détection des infractions terroristes ou d'autres infractions pénales graves, ou aux enquêtes en la matière". Elle suit également la logique de l'art. 14 OEES (par encore en vigueur), qui contient une formulation similaire.

L'*al. 2* s'appuie sur l'art. 22, par. 3, des règlements IOP de l'UE, selon lequel l'accès complet aux données figurant dans l'EES, ETIAS et le C-VIS à des fins de prévention ou de détection des

infractions terroristes ou d'autres infractions pénales graves, ou d'enquêtes en la matière, est soumis aux conditions et aux procédures fixées pour les différents systèmes d'information. Plus précisément, il s'agit des conditions et des procédures définies aux art. [...] de l'ordonnance du [...] sur le système d'entrée et de sortie (OEES; let. a), art. [...] de l'ordonnance du [...] sur le Système européen d'autorisation et d'information concernant les voyages (let. b) et art. [...] de l'ordonnance du 18 décembre 2013 sur le système central d'information sur les visas et sur le système national d'information sur les visas (OVIS; let. c). Les articles seront précisés ultérieurement, les ordonnances d'exécution concernées étant en cours d'élaboration.

Art. 15

Cet article règle la conservation des données dans le CIR. En vertu de l'art. 23 des règlements IOP de l'UE, les données figurant dans le CIR sont automatiquement effacées conformément aux dispositions relatives à la conservation des données pertinentes pour le système d'information de l'UE dont elles proviennent. Les dossiers individuels ne sont enregistrés dans le CIR qu'aussi longtemps que les données correspondantes le sont dans au moins l'un des systèmes d'information de l'UE. Il est à prévoir que les dossiers du CIR qui renvoient à des données de l'EES, d'ETIAS, du C-VIS ou d'Eurodac soient mis à jour lorsque des données sont modifiées dans les systèmes correspondants. La création d'un lien n'affectera pas la durée de conservation des données reliées par le lien.

Art. 16

Cet article règle la tenue de registres sur les consultations dans le CIR par l'autorité qui procède à la recherche. Doivent être consignées dans ce registre les informations suivantes: l'autorité qui consulte le système (let. a), les systèmes d'information Schengen-Dublin consultés (let. b), la date et l'heure de la recherche (let. c), les données utilisées pour effectuer la recherche (let. d) et les résultats de la recherche (let. e). Cette obligation est régie par l'art. 24, par. 5, des règlements IOP de l'UE, la structure de la liste étant calquée sur celle de l'art. 7 de l'ordonnance. Consigner ces informations dans un registre permet de s'assurer que les droits concédés aux personnes concernées à la section 6 de l'ordonnance sont effectivement respectés. Il convient notamment de garantir la surveillance du traitement des données conformément à l'art. 30 de l'ordonnance. Il n'existe pas d'actes d'exécution spécifiques relatifs à la tenue de registres dans le CIR. Les "résultats de la recherche" au sens de la let. e désignent les informations sur les systèmes d'information Schengen-Dublin dont les données du CIR sont issues; aucune donnée personnelle ne peut être consignée dans un registre à titre de résultats de la recherche.

Art. 17

Cet article règle le droit à l'information des personnes concernées concernant les données enregistrées dans le CIR. La base légale se trouve à l'art. 47 des règlements IOP de l'UE. Cet article prévoit que l'autorité qui saisit les données personnelles à enregistrer dans le sBMS, le CIR ou le MID fournit aux personnes concernées dans un langage clair et simple les informations visées aux art. 12 et 13 de la directive (UE) 2016/680[12] et 15 et 16 du règlement (UE) 2018/1725[13] [14]. Contrairement au CIR et au MID, le sBMS n'est pas un "fichier", autrement dit une banque de données, au sens de l'art. 3, let. g, LPD. Les modèles biométriques stockés dans le sBMS ne constituent pas des données biométriques à caractère personnel; ce système ne contient par ailleurs aucune autre donnée personnelle (cf. art. 2 de l'ordonnance sur le traitement des données signalétiques biométriques[15]). Étant donné qu'aucune donnée à caractère personnel n'est enregistrée dans le sBMS (uniquement des modèles biométriques) et que le droit à l'information sur les données enregistrées dans le MID est réglé à l'art. 24, al. 3, de l'ordonnance, la référence au CIR dans cet article est suffisante. Afin de faciliter le flux d'information avec la personne concernée, un portail en ligne sera créé conformément à l'art. 49 des règlements IOP de l'UE.

Section 4

L'ESP permet aux autorités compétentes, selon leurs droits d'accès, d'accéder rapidement, efficacement, systématiquement, sans interruptions et de façon contrôlée aux différents systèmes d'information Schengen-Dublin et aux bases de données d'Interpol. Les autorités compétentes peuvent obtenir simultanément en une seule recherche toutes les informations pertinentes auxquelles elles ont le droit d'accéder provenant de plusieurs systèmes d'information. Une recherche peut être effectuée via l'ESP à l'aide de données d'identité, de données de documents de voyage et de données biométriques à caractère personnel.

Art. 18

Les droits de consultation de l'ESP ne doivent pas être réglés dans l'ordonnance N-IOP, mais dans les ordonnances nationales sur les différents systèmes d'information. L'*al. 1* fait donc réfé-

[12] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016, p. 89

[13] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE, JO L 295 du 21.11.2018, p. 39

[14] Le règlement (UE) 2016/679 également mentionné à l'art. 47 des règlements IOP de l'UE ne fait pas partie de l'acquis de Schengen et ne s'applique donc pas à la Suisse.

[15] RS **361.3**

rence concernant les droits d'accès des autorités qui peuvent consulter l'ESP aux articles pertinents de l'OEES, de l'ordonnance sur le Système européen d'autorisation et d'information concernant les voyages, de l'OVIS (RS *142.512*) et de l'ordonnance N-SIS (RS *362.0*). En effet, les autorités qui, en vertu des art. 110*e*, al. 2, LEI et 16*b*, al. 2, LSIP, ont accès à au moins l'un des systèmes d'information peuvent consulter en ligne l'ESP. Afin qu'une autorité puisse effectuer une recherche via l'ESP, elle doit être autorisée à accéder à au moins l'un des systèmes d'information Schengen-Dublin figurant dans les articles susmentionnés ou l'une des bases de données d'Interpol. Le règlement Eurodac révisé n'ayant pas encore été repris, il n'est pour l'instant pas nécessaire de mentionner Eurodac. L'OEES et l'ordonnance sur le Système européen d'autorisation et d'information concernant les voyages étant en cours d'élaboration, les articles pertinents seront précisés en temps voulu.

L'*al. 2* renvoie, concernant les autres modalités, aux art. 7 et 9 des règlements IOP de l'UE. Il est ainsi clairement établi que les deux règlements IOP de l'UE servent de base pour accéder à des données via l'ESP. Les deux articles susmentionnés délimitent l'utilisation de l'ESP et la consultation en ligne de ce dernier. Il est essentiel que les autorités autorisées ne puissent accéder à l'ESP et aux données qu'il contient que pour les objectifs et les finalités fixés dans les instruments juridiques qui régissent les systèmes d'information et les deux règlements IOP de l'UE. L'ESP ne fournit que des données provenant des systèmes d'information de l'UE et des bases de données d'Interpol auxquels l'autorité effectuant la recherche est habilitée à accéder.

Art. 19

L'*al. 1* définit les informations pouvant être obtenues par une autorité habilitée à consulter l'ESP. Lorsqu'une recherche aboutit à un résultat positif, la réponse de l'ESP contient une indication que les données ont été trouvées (let. a), dans la mesure où aucune recherche au sens de l'art. 10 n'est menée, une référence au système d'information Schengen-Dublin ou à ses composants contenant les informations concernées (let. b) et les données contenues dans le système d'information concerné (let. c). La base légale à cet égard se trouve à l'art. 9, par. 4, des règlements IOP de l'UE, selon lequel la réponse contient les données des systèmes d'information auxquels l'autorité a accès et indique de quel système d'information de l'UE ou de quelle base de données proviennent les données concernées. Selon ce même article, une référence au sens de l'art. 19, al. 1, let. b, n'est toutefois pas fournie en cas de consultation du CIR à des fins d'identification conformément à l'art. 10 de l'ordonnance. L'art. 4, par. 2, des décisions d'exécution en vertu de l'art. 9, par. 7, des règlements IOP de l'UE[16] définit le contenu susmentionné de la réponse fournie

[16] Décision d'exécution de la Commission du 6.9.2021 précisant la procédure technique permettant au portail de recherche européen d'interroger les systèmes d'information de l'UE, les données d'Europol et les bases de données d'Interpol et déterminant le

par l'ESP.

L'*al. 2* décrit la procédure si aucune donnée n'est trouvée lors d'une recherche dans l'ESP. Dans ce cas, l'ESP informe l'autorité qui a effectué la recherche que la recherche s'est déroulée correctement mais qu'aucune donnée n'a été trouvée. Si une erreur se produit lors de la recherche, la réponse de l'ESP indiquera de quel type d'erreur il s'agit. La base légale se trouve à l'art. 4, par. 3, des décisions d'exécution précitées, qui impose cette obligation.

Art. 20

L'*al. 1* établit que toute consultation de données via l'ESP doit être consignée dans un registre. La Confédération doit tenir les registres, l'autorité responsable étant celle qui consulte le système d'information Schengen-Dublin sous-jacent. Les informations à consigner dans un registre sont les suivantes: les indications sur l'utilisateur accédant à l'ESP et sur son profil d'utilisateur (let. a), les systèmes d'information Schengen-Dublin consultés et leurs composants (let. b), la date et l'heure de la recherche (let. c) et le résultat de la recherche (let. d). Cette obligation est régie par l'art. 10 des règlements IOP de l'UE. Cette obligation est précisée à l'art. 5, par. 2, des décisions d'exécution en vertu de l'art. 9, par. 7, des règlements IOP de l'UE[17], qui énumère les informations à consigner. La tenue de ces registres vise à garantir que les droits concédés aux personnes concernées à la section 6 de l'ordonnance seront effectivement respectés. Il conviendra notamment de garantir la surveillance du traitement des données conformément à l'art. 30 de l'ordonnance.

L'*al. 2* précise que les modalités de la tenue de registres sont régies par l'art. 10, par. 3, des règlements IOP de l'UE. Cela permet de s'assurer que les registres ne seront utilisés que pour effectuer le contrôle en matière de protection des données, y compris vérifier la recevabilité d'une consultation et la licéité du traitement des données, et garantir la sécurité et l'intégrité des données. En outre, ces registres doivent être protégés de tout accès indu par des mesures appropriées et être effacés un an après leur création. Ce délai d'effacement ne s'applique pas si une procédure de contrôle a déjà été effectuée. Dans ce cas, les registres sont effacés dès qu'ils ne sont plus nécessaires à la procédure de contrôle.

Section 5

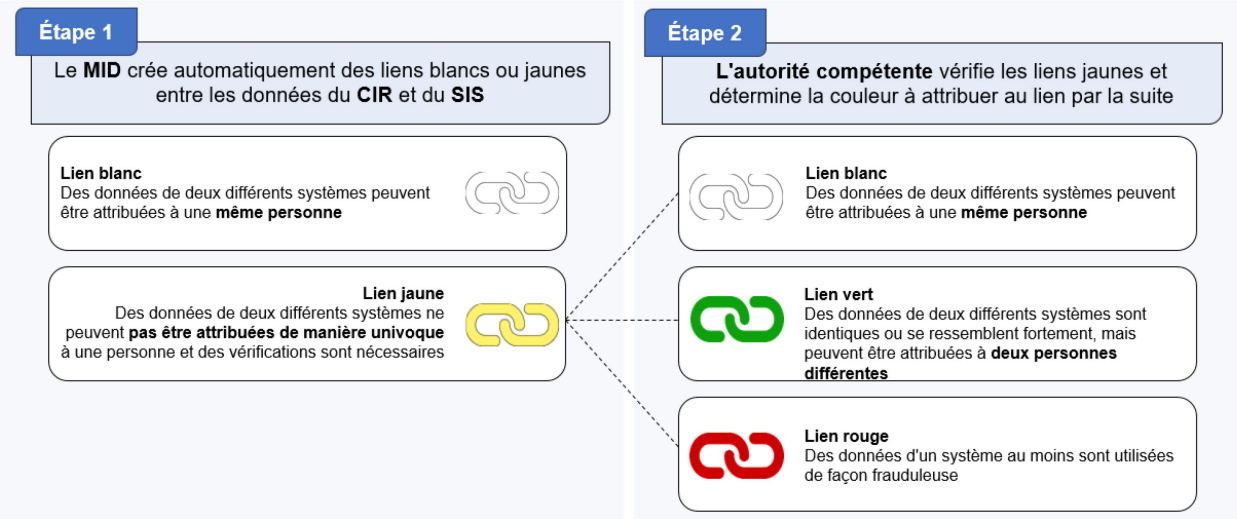
Le MID doit faciliter les contrôles d'identité et soutenir la lutte contre la fraude à l'identité. Il doit

---

format des réponses du portail de recherche européen, en vertu de l'article 9, paragraphe 7, du règlement (UE) 2019/818 du Parlement européen et du Conseil, C(2021) 6484 final; décision d'exécution de la Commission du 6.9.2021 précisant la procédure technique permettant au portail de recherche européen d'interroger les systèmes d'information de l'UE, les données d'Europol et les bases de données d'Interpol et déterminant le format des réponses du portail de recherche européen, en vertu de l'article 9, paragraphe 7, du règlement (UE) 2019/817 du Parlement européen et du Conseil, C(2021) 6486 final

[17] Ibid.

contribuer à identifier les personnes qui utilisent plusieurs identités ou de fausses identités. À cette fin, il compare les données enregistrées dans le CIR avec celles du SIS. Le MID s'appuie sur le sBMS pour la comparaison des données biométriques, alors que la comparaison des données d'identité et des données de documents de voyage est réalisée via l'ESP. Le MID est réglé dans le droit national aux art. 110*f* et 110*g* LEI et 16*c* et 16*d* LSIP.



Art. 21

Cet article prévoit que le SEM et fedpol sont responsables du traitement des données dans le MID. Selon l'art. 40, par. 3, let. b, des règlements IOP de l'UE, qui constitue la base légale, les autorités des États membres qui ajoutent des données dans le dossier de confirmation d'identité ou en modifient les données sont responsables du traitement des données dans le MID. Le SEM est compétent s'agissant des données qui proviennent du VIS, de l'EES et d'ETIAS. Si en revanche il s'agit de données issues du N-SIS, la responsabilité reviendra à fedpol.

Art. 22

L'*al. 1* fait référence, concernant le déroulement de la détection d'identités multiples, à l'art. 27 des règlements IOP de l'UE. Il décrit comment se déroule cette détection. Ce processus est lancé lors de chaque saisie ou mise à jour de données dans l'un des systèmes d'information Schengen-Dublin (VIS, SIS, ETIAS, EES, Eurodac). Pour ce faire, les nouvelles données sont comparées avec celles figurant déjà dans le CIR et le SIS. Le sBMS sert à la comparaison des données biométriques et l'ESP à celle des données d'identité et des données de documents de voyage.

L'*al. 2* fait référence à l'art. 28, par. 3 et 4, des règlements IOP de l'UE concernant les éventuels liens à établir. Si, lors d'une détection d'identités multiples, une ou plusieurs correspondances sont trouvées, des liens sont alors établis entre les nouvelles données ou les données mises à

jour utilisées pour effectuer la consultation et les données figurant déjà dans l'un des autres systèmes d'information de l'UE. Si les données d'identité, les données de documents de voyage et les données biométriques dans les dossiers liés sont les mêmes ou similaires, un lien blanc sera créé automatiquement au sens de l'art. 2, let. d, de l'ordonnance (let. a). Par contre, si ces données ne peuvent pas être considérées comme similaires, un lien jaune est créé au sens de l'art. 2, let. a, de l'ordonnance (let. b), qu'il convient ensuite de vérifier manuellement (cf. art. 23 de l'ordonnance).

Art. 23

Cet article décrit la procédure de vérification manuelle d'un lien jaune. Une vérification manuelle doit être effectuée lorsque des liens sont établis entre des données issues de différents systèmes et que les identités ne sont ni les mêmes ni similaires (liens jaunes, art. 28, par. 4, des règlements IOP de l'UE). Concernant la procédure applicable, la Commission adopte des actes délégués conformément à l'art. 28, par. 5, des règlements IOP de l'UE. La responsabilité de la vérification manuelle revient à l'autorité qui saisit ou met à jour les données dans les systèmes d'information Schengen-Dublin selon l'art. 110*g*, al. 2, LEI. Les liens vers des signalements dans le SIS qui relèvent de la police sont du ressort du bureau SIRENE. La base légale à cet égard est l'art. 110*f*, al. 2, LEI. Afin de soutenir la vérification manuelle des liens MID, un service central d'expertise sera créé en Suisse. Ce service devra apporter son soutien aux autorités dans des cas particulièrement complexes ou lorsqu'une autorité ne possède pas l'expertise nécessaire pour procéder à la vérification d'un lien MID. Il se composera de collaborateurs des offices fédéraux. La procédure de vérification manuelle est régie par l'art. 29, par. 3 à 5, des règlements IOP de l'UE. Ainsi, la vérification manuelle des différentes identités est effectuée sans délai, l'autorité qui en est responsable devant classer le lien comme vert, rouge ou blanc conformément aux art. 31 à 33 des règlements IOP de l'UE. En application de l'art. 29, par. 4, du règlement (UE) 2019/817, la vérification manuelle de différentes identités est réalisée en présence de la personne concernée. Cette dernière a la possibilité de s'exprimer devant l'autorité compétente. Si la vérification manuelle de différentes identités a lieu à la frontière, elle est effectuée, dans la mesure du possible, dans les douze heures après l'établissement du lien jaune. Si un *lien vert* est créé, celui-ci indique que même si les données d'identité liées n'appartiennent pas à la même personne, elles ne sont toutefois pas utilisées de manière illicite. Cela peut notamment être le cas lorsque les données liées comportent des données biométriques différentes mais les mêmes données d'identité, car deux personnes ont par hasard le même nom et la même date de naissance. Si un lien vert est établi, le contrôle d'identité des personnes concernées voyageant légalement en est facilité, car elles ne doivent pas être retenues inutilement à la douane afin d'établir clairement leur identité. Un *lien rouge* est par contre créé en cas d'identités multiples illicites ou de fraude à l'identité, par exemple lorsqu'une personne utilise plusieurs identités différentes, le document de voyage d'une

autre personne ou se fait passer pour une autre. Enfin, un *lien blanc* est établi lorsque les données liées désignent une seule et même personne et que cette personne figure déjà dans au moins un autre système d'information de l'UE. La mobilité des personnes qui, par exemple, sont légalement titulaires de plusieurs documents de voyage valables s'en trouve ainsi facilitée.

Art. 24

Cet article définit qui a accès aux données reliées par des liens rouges, blancs ou verts. Selon l'*al. 1*, en cas de lien rouge, il s'agira des autorités ayant accès à au moins l'un des deux systèmes d'information visés aux art. 110*a* LEI ou 16*a* LSIP. Elles pourront consulter les données enregistrées dans le dossier de confirmation d'identité conformément à l'art. 34, let. a et b, des règlements IOP de l'UE ou 26, let. a et b, de l'ordonnance (cf. les explications de l'art. 26 ci-après, qui règle le dossier de confirmation d'identité). La base légale à cet égard se trouve à l'art. 26, par. 2, des règlements IOP de l'UE.

Selon l'*al. 2*, en cas de lien blanc, les autorités ayant accès aux deux systèmes d'information visés à l'art. 110*a* LEI ou 16*a* LSIP pourront consulter les données figurant dans le dossier de confirmation d'identité (cf. les explications de l'art. 26). La base légale à cet égard est l'art. 26, par. 3, des règlements IOP de l'UE, qui règle l'accès aux liens blancs. Il faut que l'autorité qui effectue la recherche ait accès aux deux systèmes d'information entre lesquels un lien blanc est établi pour accéder aux données concernées.

L'*al. 3* règle l'accès aux données reliées par un lien vert. Les autorités ayant accès aux deux systèmes d'information visés à l'art. 110*a* LEI ou 16*a* LSIP peuvent consulter les données visées à l'art. 26 s'il y a une correspondance entre les données liées. Il faut que l'autorité qui effectue la recherche ait accès aux deux systèmes d'information entre lesquels un lien vert est établi pour accéder aux données concernées. C'est ce que prévoit l'art. 26, par. 4, des règlements IOP de l'UE. Concernant les données précises pouvant être consultées en cas de lien vert, il est possible de se référer à l'art. 34 des deux règlements IOP de l'UE ou 26 de l'ordonnance (en particulier, son al. 2), qui fournissent des explications sur le dossier de confirmation d'identité.

Art. 25

Cet article fixe la suite du processus après la vérification manuelle d'un lien jaune au sens de l'art. 22 de l'ordonnance et précise qu'en cas d'établissement d'un lien rouge ou blanc, la personne concernée doit en être informée conformément aux art. 32, par. 4 et 5, et 33, par. 4, des règlements IOP de l'UE. Ainsi, l'autorité responsable de la vérification manuelle des différentes identités informe la personne concernée de l'existence de données d'identité similaires ou différentes. Elle lui fournit en outre les informations suivantes: le numéro d'identification unique qui

figure dans le dossier de confirmation d'identité visé à l'art. 26 de l'ordonnance, le nom de l'autorité responsable de la vérification manuelle des différentes identités et l'adresse du portail en ligne créé conformément à l'art. 49 des deux règlements IOP de l'UE. L'autorité peut renoncer à l'informer pour protéger la sécurité et l'ordre publics, pour prévenir la criminalité et pour garantir qu'aucune enquête nationale ne sera compromise par la création d'un lien rouge, ou s'il existe un lien avec des signalements dans le SIS conformément aux règlements (UE) 2018/1860, (UE) 2018/1861 et (UE) 2018/1862. Elle communique par écrit au moyen d'un formulaire type les informations susmentionnées à la personne concernée. Les formulaires types figurent aux annexes des décisions d'exécution établissant un formulaire type destiné à informer les personnes de la création d'un lien rouge ou blanc[18].

L'*al. 2* règle la procédure si des éléments suggèrent qu'un lien rouge ou blanc a été enregistré de manière incorrecte, traité de manière illicite ou qu'il n'est plus à jour. Dans ce cas, la procédure est régie par les art. 32, par. 7, et 33, par. 5, des règlements IOP de l'UE. Cette procédure ne sera pas la même selon qu'il s'agit d'un lien rouge ou blanc. Si une autorité ayant accès au CIR ou au SIS dispose d'une preuve montrant qu'un lien rouge a été établi de manière incorrecte dans le MID, elle vérifie les données concernées enregistrées dans le CIR et le SIS. Si ce lien rouge est établi vers un signalement dans le SIS au sens de l'art. 29, par. 2, des règlements IOP de l'UE, l'autorité en informe le Bureau SIRENE suisse, qui prend à son tour immédiatement contact avec le Bureau SIRENE compétent de l'État membre qui a créé le signalement SIS. Ce dernier vérifie sans délai la preuve et procède, le cas échéant, à la rectification ou à la suppression du lien. Dans tous les autres cas, l'autorité compétente rectifie ou supprime le lien erroné dans le MID. Si une autorité ayant accès au CIR dispose d'une preuve montrant qu'un lien blanc a été établi de manière incorrecte dans le MID, elle doit vérifier les données concernées figurant dans le CIR ou le SIS et, le cas échéant, rectifier ou supprimer sans délai le lien dans le MID.

L'*al. 3* règle le droit à l'information concernant les données contenues dans le MID. La base légale se trouve à l'art. 47 des règlements IOP de l'UE. Cette disposition prévoit que l'autorité qui saisit les données personnelles à enregistrer dans le sBMS, le CIR ou le MID, fournit aux personnes concernées dans un langage clair et simple les informations prescrites aux art. 12 et 13 de la

[18] Annexe de la décision d'exécution de la Commission établissant un formulaire type destiné à informer les personnes de la création d'un lien rouge conformément au règlement (UE) 2019/818 du Parlement européen et du Conseil, C(2021) 5989 final; annexe de la décision d'exécution de la Commission établissant un formulaire type destiné à informer les personnes de la création d'un lien rouge conformément au règlement (UE) 2019/817 du Parlement européen et du Conseil, C(2021) 5988 final; annexe de la décision d'exécution de la Commission établissant un formulaire type destiné à informer les personnes de la création d'un lien blanc conformément au règlement (UE) 2019/817 du Parlement européen et du Conseil, C(2021) 5620 final; annexe de la décision d'exécution de la Commission établissant un formulaire type destiné à informer les personnes de la création d'un lien blanc conformément au règlement (UE) 2019/818 du Parlement européen et du Conseil, C(2021) 5619 final

directive (UE) 2016/680[19] ainsi que 15 et 16 du règlement (UE) 2018/1725[20] [21]. Étant donné qu'aucune donnée personnelle n'est enregistrée dans le sBMS (uniquement des modèles biométriques – celui-ci n'étant pas un "fichier", autrement dit une banque de données, au sens de l'art. 3, let. g, LPD – et que le droit à l'information concernant des données figurant dans le CIR est réglé à l'art. 17 de l'ordonnance, la référence au MID à l'al. 3 est suffisante. Afin de faciliter le flux d'information avec la personne concernée, un portail en ligne est créé conformément à l'art. 49 des règlements IOP de l'UE.

Art. 26

L'*al. 1* règle le contenu du dossier de confirmation d'identité. Si la détection d'identités multiples déclenche un lien entre des données du SIS, de l'EES, d'ETIAS, du C-VIS ou d'Eurodac, un dossier de confirmation d'identité est créé. La base légale à cet égard se trouve aux art. 110*f*, al. 4, LEI et 34 des règlements IOP de l'UE. Le dossier de confirmation d'identité contient les données suivantes: le type de lien établi entre les données, à savoir un lien jaune, vert, rouge ou blanc (let. a), la référence aux systèmes d'information Schengen-Dublin dont sont issues les données liées (let. b), le numéro d'identification unique permettant d'extraire les données liées des systèmes d'information Schengen-Dublin correspondants (let. c), l'autorité responsable de la vérification manuelle des différentes identités (let. d) et la date de création du lien ou toute mise à jour de celui-ci (let. e).

L'*al. 2* renvoie à l'annexe 2 de l'ordonnance, qui contient le catalogue de données du dossier de confirmation d'identité du MID. La matrice des droits d'accès qui y figure repose sur les art. 23 et 24 de l'ordonnance qui règlent respectivement la vérification manuelle d'un lien jaune et l'accès à des données issues de liens. Ainsi, les autorités responsables de la vérification manuelle des différentes identités peuvent consulter le dossier de confirmation d'identité, y compris le lien jaune (cf. art. 110*g*, al. 2, en relation avec l'art. 110*f*, al. 2 et 4, LEI). Les autorités ayant accès à au moins l'un des systèmes d'information au sens de l'art. 110*a* LEI ou 16*a* LSIP, entre lesquels un lien rouge existe, peuvent consulter les données enregistrées dans le dossier de confirmation d'identité visé à l'art. 34, let. a et b, des règlements IOP de l'UE ou 26, al. 1 et 2, de l'ordonnance (art. 24, al. 1). De même, les autorités qui ont accès aux systèmes d'information visés à l'art. 110*a*

[19] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016, p. 89; modifié en dernier lieu par le rectificatif à la directive (UE) 2016/680, JO L 74 du 4.3.2021, p. 36

[20] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, JO L 295 du 21.11.2018, p. 39

[21] Le règlement (UE) 2016/679 également cité ne faisant pas partie de l'acquis de Schengen, il ne lie pas la Suisse.

LEI ou 16*a* LSIP, entre lesquels un lien blanc a été établi, peuvent consulter le dossier de confirmation d'identité prévu à l'art. 26 de l'ordonnance (art. 24, al. 2). Enfin, les autorités ayant accès aux systèmes d'information visés à l'art. 110*a* LEI ou 16*a* LSIP, entre lesquels un lien vert a été établi, peuvent consulter le dossier de confirmation d'identité prévu à l'art. 26 de l'ordonnance si une recherche a abouti à une correspondance entre les données liées (art. 24, al. 3). Les droits d'accès aux données conformément à l'al. 1 susmentionnés sont détaillés à l'annexe 2.

Art. 27

Cet article traite de la conservation des données dans les dossiers de confirmation d'identité. Conformément aux indications relatives au sBMS et au CIR (cf. les explications des art. 6 et 15), les dossiers de confirmation d'identité et les données qu'ils contiennent ne sont conservés qu'aussi longtemps que les données liées demeurent enregistrées dans les systèmes d'information sous-jacents. Ils sont automatiquement supprimés du MID. Cette disposition reprend le contenu normatif de l'art. 35 des règlements IOP de l'UE.

Art. 28

Cet article règle la tenue de registres sur les consultations du MID. Chaque consultation du MID doit être consignée dans un registre. La Confédération doit tenir les registres, l'autorité responsable étant celle qui consulte le système d'information Schengen-Dublin sous-jacent. Cette obligation découle de l'art. 36, par. 2, des règlements IOP de l'UE. Par conséquent, tout État membre tient des registres sur les consultations effectuées par les autorités auxquelles il a accordé des droits d'accès. La tenue de ces registres vise à garantir que les droits concédés aux personnes concernées à la section 6 de l'ordonnance seront effectivement respectés. L'autorité qui effectue la recherche doit consigner dans un registre les informations suivantes: l'utilisateur qui entreprend la recherche (let. a), le but visé par cet accès (let. b), la date et l'heure de la recherche (let. c) et les données utilisées pour effectuer la recherche (let. d).

Section 6

La section 6 règle les droits des personnes qui figurent dans les systèmes d'information Schengen-Dublin et leurs composants.

Art. 29

L'*al. 1* règle le droit des personnes figurant dans les systèmes d'information Schengen-Dublin à accéder aux données les concernant et à les faire rectifier ou effacer. Il renvoie à cette fin aux ordonnances relatives aux systèmes contenant ces données. Concernant les entrées dans le N-SIS, la procédure à suivre est régie par les art. 50 et 51 de l'ordonnance N-SIS (let. a). De même, concernant les entrées dans le C-VIS, l'EES et ETIAS, la procédure est régie par l'ordonnance

relative au système concerné. Ces trois ordonnances sont en cours d'élaboration, raison pour laquelle les dispositions ad hoc de l'ordonnance N-IOP seront complétées ultérieurement. Une référence à Eurodac n'est actuellement pas nécessaire, étant donné que le règlement Eurodac révisé n'a pas encore été repris.

L'*al. 2* précise que les demandes d'accès à des données, de rectification ou d'effacement de liens et de données dans le MID ou de données dans le CIR doivent être adressées par écrit au SEM. Cette disposition se fonde sur les art. 8 et 21 de l'ordonnance, qui règlent la responsabilité du traitement de données dans le CIR et le MID. Selon ces dispositions, le SEM est responsable du traitement des données dans le CIR. Il l'est également du traitement des données dans le MID, dans la mesure où il ajoute ou modifie dans le dossier de confirmation d'identité des données concernant les systèmes d'information qu'il exploite. C'est pourquoi il est justifié de désigner le SEM comme point de contact pour les demandes d'accès à des données, de rectification ou d'effacement de liens et de données dans le MID ou de données dans le CIR. En effet, il est à prévoir que la plupart des liens dans le MID concerneront *exclusivement* des systèmes d'information du SEM (VIS, EES, ETIAS). Concrètement, la demande écrite doit être adressée au service central d'expertise MID rattaché au SEM, qui sera créé afin de soutenir la vérification manuelle des liens MID. Si l'examen du service d'expertise révèle qu'une autre autorité que le SEM est compétente (c.-à-d. dans les cas où le N-SIS est concerné), il entre en contact avec cette autorité. Cette dernière vérifie alors les motifs et, le cas échéant, rectifie ou efface les liens ou les données concernés dans le MID, ou les données dans le CIR. Le SEM se charge ensuite de fournir des informations à la personne ayant déposé la demande (cf. à ce sujet l'al. 3).

L'*al. 3* spécifie que le SEM traite les demandes conformément à l'al. 2 après concertation avec l'autorité compétente qui a saisi ou fait saisir les données en question. Tandis que le SEM est responsable du traitement des données dans le CIR (art. 8), le SEM et fedpol sont responsables du traitement des données dans le MID (art. 21). En cas de lien MID avec le SIS, le SEM se concerte avec fedpol. Dans les autres cas, la concertation a lieu avec les services compétents du SEM. Cela permet de garantir que les motifs d'une saisie soient suffisamment connus.

L'*al. 4* prévoit qu'une personne dont les données personnelles sont enregistrées dans le MID peut en demander la rectification ou l'effacement conformément à l'art. 48 des règlements IOP de l'UE. La demande contient les informations nécessaires à l'identification de la personne concernée (ces informations ne peuvent être utilisées que pour permettre à la personne concernée d'exercer ses droits et doivent être effacées immédiatement après). La responsabilité de la vérification et, le cas échéant, de la rectification ou de l'effacement des demandes revient à l'autorité chargée de la vérification manuelle des liens jaunes visée à l'art. 22 de l'ordonnance. Si des données sont rectifiées ou effacées, la personne concernée en est informée par écrit. Si l'autorité chargée de

la vérification d'un lien jaune n'estime pas que les données stockées dans le MID sont erronées ou qu'elles y ont été enregistrées de façon illicite, elle rend une décision sujette à recours, dans laquelle elle indique les raisons pour lesquelles elle n'est pas disposée à rectifier ou à effacer les données. La décision doit indiquer les voies de droit; les voies de droit ordinaires sont applicables en l'espèce.

Art. 30

L'*al. 1* détermine que les autorités cantonales de protection des données et le Préposé fédéral à la protection des données et à la transparence (PFPDT) collaborent dans le cadre de leurs compétences respectives et coordonnent la surveillance du traitement des données personnelles. Il se fonde sur l'art. 51 des règlements IOP de l'UE, qui prescrivent que des autorités de surveillance indépendantes contrôlent la licéité du traitement des données personnelles dans le cadre de l'interopérabilité. En Suisse, cette responsabilité revient aux autorités cantonales de protection des données et au PFPDT.

L'*al. 2* prévoit que le PFPDT collabore avec le Contrôleur européen de la protection des données dans l'exercice de ses tâches. Il est le point de contact national de ce dernier. Cette disposition se fonde sur l'art. 22 de l'OEES, qui est en cours d'élaboration.

L'*al. 3* renvoie à l'art. 51 des règlements IOP de l'UE concernant les autres précisions. Il établit ainsi clairement que ces deux règlements européens constituent la base de la surveillance du traitement des données. Le PFPDT garantit entre autres que les processus de traitement des données personnelles soient contrôlés au moins une fois tous les quatre ans par les autorités nationales compétentes. Il publie chaque année le nombre de demandes de rectification, d'effacement ou de limitation du traitement des données personnelles, les mesures subséquentes prises et le nombre de ces mesures exécutées à la demande des personnes concernées.

Section 7

La section 7 fournit des informations sur la sécurité des données.

Art. 31

L'*al. 1* règle la sécurité des données. Il détermine que la garantie de la sécurité des données est régie par l'ordonnance du 25 novembre 2020 sur la transformation numérique et l'informatique (OTNI; RS *172.010.58*) et par l'ordonnance du 27 mai 2020 sur les cyberrisques (OPCy; RS *120.73*). À cet égard, il convient également de se référer à l'art. 42, par. 1 et 4, des règlements IOP de l'UE, qui porte sur la sécurité du traitement des données personnelles.

L'*al. 2* vise à assurer que les autorités qui ont accès aux composants d'interopérabilité prennent

les mesures organisationnelles et techniques nécessaires selon la législation relative à la protection des données pour empêcher les tiers non autorisés d'accéder aux données. Ces mesures doivent correspondre à celles visées à l'art. 42, par. 3, des règlements IOP de l'UE (cf. à ce sujet l'art. 42, par. 2, de ces mêmes règlements).

Section 8

La section 8 règle à l'art. 32 l'entrée en vigueur de l'ordonnance, dont la date sera complétée ultérieurement.

3. Modifications à venir d'autres ordonnances

3.1. Ordonnances régissant les systèmes d'information Schengen-Dublin

Plusieurs ordonnances portant sur des systèmes d'information Schengen-Dublin doivent être modifiées dans le cadre du projet d'interopérabilité. Il s'agira notamment de déterminer dans l'ordonnance nationale OEES quelles données doivent être également enregistrées dans le CIR et quand les données doivent être effacées. L'ordonnance nationale ETIAS nécessite elle aussi une modification concernant les données devant également être enregistrées dans le CIR. Cette ordonnance sera élaborée prochainement et devrait entrer en vigueur en décembre 2022. En outre, l'ordonnance nationale VIS devra être modifiée dans un avenir proche, là aussi en ce qui concerne les données à enregistrer dans le CIR. Enfin, le projet de remaniement d'Eurodac rendra ce système interopérable avec les autres systèmes d'information: une ordonnance nationale Eurodac comprenant toutes les dispositions pertinentes en matière d'interopérabilité sera mise au point. Le développement d'Eurodac fait actuellement partie du pacte européen sur la migration et l'asile et devait être approuvé en même temps que ce dernier à l'échelon européen. Par la suite, on a abordé la possibilité de séparer le projet du pacte, ce qui permettrait une entrée en vigueur plus rapide de l'interopérabilité avec Eurodac. Les ordonnances citées ci-dessus devront également prévoir une nouvelle procédure pour l'accès des autorités de poursuite pénale aux systèmes EES, VIS et ETIAS suite à une consultation du CIR. Les ordonnances seront modifiées de façon à ce que les deux possibilités de consultation soient possibles. La consultation du CIR est cependant considérée comme prioritaire. Étant donné que les ordonnances en question sont pour certaines encore inexistantes, il n'est pas possible actuellement de dresser une liste exhaustive des modifications d'ordonnance qui s'imposent. Celles-ci seront cependant minimes.

3.2. Autres ordonnances

D'autres ordonnances nécessitent également une modification pour permettre l'interopérabilité. Il est prévu de modifier l'art. 19, al. 1, de l'ordonnance du 12 avril 2006 SYMIC (RS *142.513*) de manière à ce qu'il ne renvoie plus à l'art. 111*f* LEI, étant donné que ce dernier sera abrogé lors de l'entrée en vigueur de la nouvelle LEI introduite par l'arrêté fédéral IOP (FF *2021* 674).

L'art. 87*a* de l'ordonnance du 24 octobre 2007 relative à l'admission, au séjour et à l'exercice d'une activité lucrative (OASA; RS *142.201*) doit être modifié de façon à ce qu'il renvoie non plus à l'art. 111*i* LEI, mais au nouvel art. 109*k* LEI, lui aussi introduit par l'arrêté fédéral IOP.

4. Conséquences sur les finances et l'état du personnel

4.1. Conséquences sur les finances et l'état du personnel de la Confédération

Il n'y a pas lieu de s'attendre à ce que les coûts liés à l'ordonnance N-IOP dépassent ce qui avait été annoncé dans le message (FF *2020* 7721, 7785 à 7790). Tant dans la phase de projet que lors de la mise en œuvre des règlements IOP de l'UE, il y a des conséquences pour la Confédération aussi bien au niveau des finances que du personnel. L'interopérabilité est un des éléments du programme de développement de l'acquis de Schengen du DFJP. Les projets de fedpol et du SEM font partie d'un crédit d'engagement pour le développement de l'acquis de Schengen/Dublin. L'ensemble des coûts des projets d'interopérabilité a été estimé à 21 millions de francs pour la période de 2020 à 2025. Les coûts d'exploitation devraient s'élever à 0,2 million en 2023 et à près de 2 millions annuels dès 2024.

Par sa décision du 12 mai 2021, le Conseil fédéral a pris acte des besoins supplémentaires en personnel occasionnés par l'interopérabilité jusqu'en 2023. Le 23 juin 2021, il a approuvé les ressources supplémentaires pour 2022 dans son évaluation globale des ressources dans le domaine du personnel 2021. Pour ce qui est des besoins en personnel pour 2023, le DFJP les réexaminera dans le cadre de l'élaboration du budget 2023. Les ressources estimées nécessaires actuellement dès 2024 feront l'objet d'une demande ultérieure au Conseil fédéral.

4.2. Conséquences sur les finances et l'état du personnel des cantons

Les autorités cantonales de migration et de police pourront bénéficier de l'interopérabilité dans leurs activités, ce qui implique néanmoins des adaptations techniques et des modifications des processus dans les systèmes d'information cantonaux. La Confédération travaille actuellement en étroite collaboration avec les cantons pour identifier les besoins en la matière. Elle compte mettre son service d'expertise MID à la disposition des cantons pour les décharger dans la vérification des identités. Les charges supplémentaires pour les cantons sont exposées plus en détail dans le message (FF *2020* 7721, 7790).

5. Aspects juridiques

5.1. Constitutionnalité

Les échanges de notes entre la Suisse et l'UE concernant la reprise des règlements IOP de l'UE

se fondent sur l'art. 54, al. 1, Cst. et ont été soumis à l'approbation de l'Assemblée fédérale[22].

Le présent projet tient compte des prescriptions du droit constitutionnel et assure notamment que les garanties constitutionnelles soient respectées (cf. section 6). Au vu des bases légales prévues et des principes de la protection des données et de la sécurité des données déjà garantis légalement, la restriction des droits fondamentaux prévue au niveau de la loi apparaît comme proportionnée au but visée (art. 36, al. 1 à 3, Cst.).

5.2. Compatibilité avec les obligations internationales de la Suisse

Les modifications d'ordonnances mentionnées sont conformes au droit international. En reprenant les deux développements de l'acquis de Schengen, la Suisse remplit ses obligations découlant de l'AAS. Elle contribue par ailleurs à l'utilisation uniforme des systèmes d'information Schengen-Dublin. La reprise des deux règlements européens et les modifications légales qu'elle induit sont ainsi conformes aux obligations internationales de la Suisse.

5.3. Forme de l'acte législatif

Lee présent projet permet de procéder aux modifications nécessaires à la mise en œuvre de l'interopérabilité au niveau de l'ordonnance. Il s'agit d'une part des modifications d'ordonnances nécessaires à la mise en œuvre des révisions législatives. D'autre part, certaines dispositions des règlements IOP de l'UE doivent être explicitées au niveau de l'ordonnance. Par ailleurs, les actes de droit tertiaire (décisions d'exécution) en matière d'interopérabilité notifiés jusqu'à présent doivent être mis en application. C'est à ces fins que l'ordonnance sur l'interopérabilité des systèmes d'information Schengen-Dublin, autrement dit l'ordonnance N-IOP, est élaborée.

6. Protection des données

En raison de l'introduction des nouveaux composants centraux qui ont une influence sur tous les systèmes d'information Schengen-Dublin, plusieurs lois ont été modifiées en conséquence, notamment en ce qui concerne la protection des données (cf. chap. 14, 14*a*, 14*b* et 14*c* LEI). Le présent projet comprend lui aussi des dispositions relatives à la protection des données (cf. sections 6 et 7).

[22] Message IOP, FF **2020** 7791 ss