



INTERPOL

*Règlement d'INTERPOL  
sur le traitement des données*

---

[III/IRPD/GA/2011 (2025)]

## RÉFÉRENCES

Règlement relatif à la coopération policière internationale et au contrôle interne des fichiers de l'O.I.P.C.-INTERPOL, adopté par l'Assemblée générale de l'Organisation en sa 51<sup>ème</sup> session (Torremolinos (Espagne), 1982) par la résolution AGN/51/RES/1.

Règlement sur la destruction des informations de police enregistrées par le Secrétariat général, adopté par le Comité exécutif en sa 84<sup>ème</sup> session (Saint-Cloud (France), 4 - 6 mars 1987), en vertu des pouvoirs qui lui ont été délégués par l'Assemblée générale en sa 55<sup>ème</sup> session par la résolution AGN/55/RES/2.

Règlement relatif à une base de données sélectionnées implantée au Secrétariat général de l'O.I.P.C.-INTERPOL et à l'accès direct des B.C.N. à celle-ci, adopté par l'Assemblée générale de l'Organisation en sa 59<sup>ème</sup> session (Ottawa (Canada), 1990) par la résolution AGN/59/RES/7.

Règlement portant sur l'accès au réseau de télécommunications et aux bases de données d'INTERPOL par une organisation intergouvernementale, adopté par l'Assemblée générale de l'Organisation en sa 70<sup>ème</sup> session (Budapest (Hongrie), 2001) par la résolution AG-2001-RES-08.

Règlement sur le traitement d'informations pour la coopération policière internationale, adopté par l'Assemblée générale de l'Organisation en sa 72<sup>ème</sup> session (Benidorm (Espagne), 2003) par la résolution AG-2003-RES-04.

Règlement d'application du Règlement sur le traitement d'informations pour la coopération policière internationale, adopté par l'Assemblée générale de l'Organisation en sa 76<sup>ème</sup> session (Marrakech (Maroc), 2007) par la résolution AG-2007-RES-09.

Règlement d'INTERPOL sur le traitement des données, adopté par l'Assemblée générale de l'Organisation en sa 80<sup>ème</sup> session (Hanoï (Viet Nam), 2011) par la résolution AG-2011-RES-07 et abrogeant à la date du 30 juin 2012 le Règlement sur le traitement d'informations pour la coopération policière internationale, le Règlement d'application du Règlement sur le traitement d'informations pour la coopération policière internationale et le Règlement portant sur l'accès au réseau de télécommunications et aux bases de données d'INTERPOL par une organisation intergouvernementale.

Le Secrétariat général a rectifié la version française du Règlement le 14 mars 2013, conformément aux dispositions de l'article 33(3) du Règlement intérieur de l'Assemblée générale de l'O.I.P.C.-INTERPOL.

Articles 1, 4, 8, 10, 13, 23, 27, 34, 40, 44, 49, 52, 53, 61, 68, 69, 81, 88, 89, 104, 105 et 126 modifiés ; l'article 70 est devenu l'article 71, un nouvel article 70 a été ajouté et l'article 71 est devenu l'article 72 ; les articles 80 et 81 ont été regroupés sous l'article 81. La version anglaise des articles 1, 27, 93 et 104 et la version arabe de l'article 82 ont été modifiées lors de la 83<sup>ème</sup> session de l'Assemblée générale (Monaco, 2014) par la résolution AG-2014-RES-18.

Articles 5, 18 et 121 modifiés, article 121A ajouté lors de la 85<sup>ème</sup> session de l'Assemblée générale (Bali (Indonésie), 2016) par la résolution AG-2016-RES-06.

Articles 13, 22, 32, 36, 37, 46, 49, 50, 51, 52, 53, 63, 69, 70, 71, 105, 125, 126 et 134 modifiés lors de la 88<sup>ème</sup> session de l'Assemblée générale (Santiago (Chili), 2019) par la résolution GA-2019-88-RES-02.

## **RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES**

Articles 1, 10, 21, 36, 64, 104, 105 et 106 modifiés, article 43A ajouté et article 65 supprimé lors de la 91<sup>ème</sup> session de l'Assemblée générale (Vienne (Autriche), 2023) par la résolution GA-2023-91-RES-08.

Articles 1, 22, 24, 42, 47, 67, 70, 71 et 135 modifiés lors de la 92<sup>ème</sup> session de l'Assemblée générale (Glasgow (Royaume-Uni), 2024) par les résolutions GA-2024-92-RES-07 et GA-2024-92-RES-08.

Article 94 supprimé lors de la 93<sup>ème</sup> session de l'Assemblée générale (Marrakech (Maroc), 2025) par la résolution GA-2025-93-RES-08.

TABLE DES MATIÈRES

<b>PRÉAMBULE .....</b>	<b>8</b>
Article 1 : Définitions.....	8
Article 2 : But.....	10
Article 3 : Objet .....	10
Article 4 : Champ d'application .....	10
<b>TITRE 1 : PRINCIPES GÉNÉRAUX.....</b>	<b>10</b>
<b>CHAPITRE I : PRINCIPES RELATIFS À LA COOPÉRATION POLICIÈRE INTERNATIONALE.....</b>	<b>10</b>
Article 5 : Respect des principes de gouvernance et responsabilités associées au traitement des données .....	10
Article 6 : Accès au Système d'information d'INTERPOL .....	10
Article 7 : Maîtrise du traitement des données .....	11
Article 8 : Recours aux notices INTERPOL et aux diffusions .....	11
Article 9 : Communication directe par voie de messages .....	11
<b>CHAPITRE II : PRINCIPES RELATIFS AU TRAITEMENT DE L'INFORMATION .....</b>	<b>11</b>
Article 10 : Finalités de la coopération policière .....	11
Article 11 : Licéité.....	12
Article 12 : Qualité.....	12
Article 13 : Transparence.....	12
Article 14 : Confidentialité .....	13
Article 15 : Sécurité .....	13
Article 16 : Traitement externe à des fins de police .....	14
Article 17 : Mise en œuvre effective .....	14
Article 18 : Droits d'accès, de rectification et d'effacement des données.....	15
<b>TITRE 2 : ACTEURS .....</b>	<b>15</b>
<b>CHAPITRE I : FONCTIONS DES BUREAUX CENTRAUX NATIONAUX .....</b>	<b>15</b>
Article 19 : Coordination des flux de données .....	15
Article 20 : Coordination des recherches criminelles .....	15
Article 21 : Délivrance des autorisations d'accès direct au plan national.....	15
<b>CHAPITRE II : FONCTIONS DU SECRÉTARIAT GÉNÉRAL .....</b>	<b>16</b>
Article 22 : Administration du système.....	16
Article 23 : Mesures supplémentaires de renforcement de la coopération .....	16
Article 24 : Enregistrement des données.....	16
Article 25 : Coordination .....	17
Article 26 : Mesures d'urgence .....	17

<b>CHAPITRE III : RELATIONS AVEC LES ENTITÉS INTERNATIONALES ET LES ENTITÉS PRIVÉES .....</b>	<b>17</b>
Article 27 : Conditions relatives au traitement des données par les entités internationales .....	17
Article 28 : Conditions relatives au traitement des données par les entités privées .....	18
<b>TITRE 3 : MODALITÉS DE TRAITEMENT DES DONNÉES.....</b>	<b>19</b>
<b>CHAPITRE I : BASES DE DONNÉES DE POLICE .....</b>	<b>19</b>
<b>SECTION 1 : AUTORISATION .....</b>	<b>19</b>
Article 29 : Création d'une base de données .....	19
Article 30 : Modification d'une base de données existante.....	20
Article 31 : Suppression d'une base de données existante.....	20
Article 32 : Autorisations accordées par le Comité exécutif .....	20
Article 33 : Registre des bases de données existantes .....	20
<b>SECTION 2 : FONCTIONNEMENT .....</b>	<b>21</b>
Article 34 : Respect du Statut de l'Organisation.....	21
Article 35 : Intérêt des données pour la coopération policière internationale.....	21
Article 36 : Caractéristiques générales des bases de données .....	21
Article 37 : Conditions minimales d'enregistrement dans les bases de données .....	22
Article 38 : Conditions supplémentaires d'enregistrement de données relatives à des personnes ....	22
Article 39 : Conditions supplémentaires d'enregistrement relatives aux personnes décédées.....	22
Article 40 : Conditions supplémentaires d'enregistrement relatives aux personnes victimes ou témoins .....	22
Article 41 : Conditions supplémentaires d'enregistrement relatives aux personnes mineures.....	23
Article 42 : Conditions supplémentaires de traitement relatives aux données particulièrement sensibles .....	23
Article 43 : Conditions supplémentaires d'enregistrement relatives aux données copiées ou téléversées.....	23
Article 43A : Conditions supplémentaires relatives au traitement temporaire de grands ensembles de données.....	23
Article 44 : Statut des personnes .....	24
Article 45 : Définition des conditions particulières d'utilisation lors de l'enregistrement .....	24
Article 46 : Mise à jour .....	25
Article 47 : Conditions supplémentaires relatives à l'enregistrement des informations accessibles au public et des informations émanant de personnes ou d'entités .....	25
Article 48 : Compléments d'information et correction.....	26
Article 49 : Durée de conservation .....	26
Article 50 : Évaluation régulière .....	26
Article 51 : Effacement de données .....	27
Article 52 : Conservation temporaire des antécédents criminels.....	27
Article 53 : Conservation des données à des fins d'orientation .....	28
<b>SECTION 3 : CONSULTATION .....</b>	<b>28</b>
Article 54 : Accès direct.....	28
Article 55 : Interconnexion .....	28

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

Article 56 : Téléchargement à des fins de coopération policière internationale .....	29
Article 57 : Accès indirect .....	30
Article 58 : Restrictions d'accès.....	30
Article 59 : Divulgation de données faisant l'objet de restrictions .....	31
Article 60 : Accès par des tiers.....	31
Article 61 : Divulgation de données au public .....	31
<b>SECTION 4 : UTILISATION .....</b>	<b>32</b>
Article 62 : Conditions d'utilisation .....	32
Article 63 : Vérification de l'exactitude et de la pertinence des données .....	32
Article 64 : Utilisation de données pour une finalité de police criminelle autre que la finalité initiale ou à une fin administrative .....	32
Article 65 : Utilisation à des fins administratives [ <i>supprimé</i> ].....	33
Article 66 : Conditions particulières d'utilisation .....	33
Article 67 : Retransmission des données .....	33
<b>SECTION 5 : RÈGLES SPÉCIFIQUES RELATIVES AUX FICHIERS D'ANALYSE CRIMINELLE .....</b>	<b>34</b>
Article 68 : Fichiers d'analyse .....	34
Article 69 : Utilisation des fichiers d'analyse .....	34
Article 70 : Conditions supplémentaires d'enregistrement de données à des fins d'analyse criminelle.....	35
Article 71 : Rapports d'analyse criminelle .....	35
Article 72 : Achèvement des projets d'analyse criminelle .....	36
<b>CHAPITRE II : NOTICES ET DIFFUSIONS.....</b>	<b>36</b>
<b>SECTION 1 : DISPOSITIONS COMMUNES AUX NOTICES .....</b>	<b>36</b>
Article 73 : Système des notices INTERPOL .....	36
Article 74 : Rôle du Secrétariat général.....	36
Article 75 : Structure des notices INTERPOL .....	36
Article 76 : Demande de publication de notice .....	37
Article 77 : Examen de la demande par le Secrétariat général.....	37
Article 78 : Demandes incomplètes ou ne répondant pas aux conditions de publication de notices.....	37
Article 79 : Publication des notices.....	37
Article 80 : Mise en œuvre des notices .....	38
Article 81 : Suspension, retrait ou annulation d'une notice .....	38
<b>SECTION 2 : DISPOSITIONS PARTICULIÈRES AUX NOTICES ROUGES.....</b>	<b>39</b>
Article 82 : But des notices rouges .....	39
Article 83 : Conditions particulières applicables à la publication des notices rouges .....	39
Article 84 : Garanties fournies par le Bureau central national ou l'entité internationale à l'origine de la notice .....	40
Article 85 : Communication de documents susceptibles de faciliter les procédures d'extradition ou de remise par le Bureau central national ou l'entité internationale à l'origine de la notice .....	40

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

Article 86 : Examen juridique par le Secrétariat général.....	40
Article 87 : Mesures à prendre en cas de localisation de la personne recherchée .....	40
<b>SECTION 3 : DISPOSITIONS PARTICULIÈRES AUX AUTRES NOTICES .....</b>	<b>41</b>
Article 88 : Notices bleues .....	41
Article 89 : Notices vertes.....	41
Article 90 : Notices jaunes.....	41
Article 91 : Notices noires.....	42
Article 92 : Notices mauves .....	42
Article 93 : Notices orange .....	43
Article 94 : Notices œuvres d'art volées [ <i>supprimé</i> ] .....	43
Article 95 : Notices spéciales INTERPOL-Conseil de sécurité des Nations Unies .....	43
Article 96 : Autres notices spéciales .....	43
<b>SECTION 4 : DIFFUSIONS .....</b>	<b>43</b>
Article 97 : Système des diffusions .....	43
Article 98 : Mise à disposition des formulaires de diffusions .....	44
Article 99 : Transmission des diffusions .....	44
Article 100 : Suspension ou retrait d'une diffusion .....	44
Article 101 : Enregistrement de demandes de coopération ou alertes transmises par voie de message .....	45
<b>SECTION 5 : NOTICES ET DIFFUSIONS À L'INITIATIVE DU SECRÉTARIAT GÉNÉRAL .....</b>	<b>45</b>
Article 102 : Sollicitations d'informations .....	45
Article 103 : Publication de notices .....	45
<b>SECTION 6 : SIGNALEMENTS POSITIFS .....</b>	<b>45</b>
Article 104 : Génération de signalements positifs .....	45
Article 105 : Procédure de traitement de signalements positifs .....	46
Article 106 : Relevés des signalements positifs .....	46
<b>CHAPITRE III : SÉCURITÉ DES DONNÉES .....</b>	<b>46</b>
<b>SECTION 1 : GESTION DES DROITS D'ACCÈS AU SYSTÈME D'INFORMATION D'INTERPOL .....</b>	<b>46</b>
Article 107 : Désignation d'un nouveau Bureau central national.....	46
Article 108 : Octroi d'un accès à une nouvelle entité nationale .....	46
Article 109 : Octroi d'un accès à une nouvelle entité internationale .....	46
Article 110 : Registre des accès au Système d'information d'INTERPOL.....	46
Article 111 : Droits d'accès individuels au Système d'information d'INTERPOL.....	47
<b>SECTION 2 : RESPECT DE LA CONFIDENTIALITÉ .....</b>	<b>47</b>
Article 112 : Niveaux de confidentialité .....	47
Article 113 : Mesures supplémentaires prises par le Secrétariat général .....	48
Article 114 : Respect de la confidentialité dans le Système d'information d'INTERPOL .....	48

---

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

<b>SECTION 3 : GESTION DU SYSTÈME DE SÉCURITÉ .....</b>	<b>48</b>
Article 115 : Règles de sécurité .....	48
Article 116 : Mise en œuvre par les Bureaux centraux nationaux et les entités .....	48
Article 117 : Désignation d'un officier de sécurité .....	49
<b>SECTION 4 : INCIDENTS DE SÉCURITÉ .....</b>	<b>49</b>
Article 118 : Information relative à un incident de sécurité .....	49
Article 119 : Restauration partielle ou totale du Système d'information d'INTERPOL .....	49
<b>TITRE 4 : CONTRÔLES.....</b>	<b>49</b>
<b>CHAPITRE I : NATURE DES CONTRÔLES .....</b>	<b>49</b>
Article 120 : Contrôle des utilisateurs .....	49
Article 121 : Désignation d'un officier délégué à la protection des données au sein des Bureaux centraux nationaux et des entités nationales et internationales .....	49
Article 121A : Désignation d'un officier délégué à la protection des données au sein du Secrétariat général.....	50
Article 122 : Contrôle de l'utilisation des données.....	51
Article 123 : Évaluation des entités nationales .....	51
Article 124 : Évaluation des Bureaux centraux nationaux.....	51
<b>CHAPITRE II : OUTILS DE CONTRÔLE.....</b>	<b>51</b>
Article 125 : Base de gestion de la conformité .....	51
Article 126 : Registre des opérations de traitement .....	52
Article 127 : Comparaison de données à des fins de vérification.....	52
<b>CHAPITRE III : MESURES DE CONTRÔLE .....</b>	<b>53</b>
Article 128 : Procédure d'examen .....	53
Article 129 : Mesures conservatoires .....	53
Article 130 : Mesures applicables aux utilisateurs .....	53
Article 131 : Mesures correctives applicables aux Bureaux centraux nationaux et aux entités internationales .....	53
<b>TITRE 5 : DISPOSITIONS FINALES .....</b>	<b>54</b>
<b>CHAPITRE I : TRAITEMENT DANS TOUT AUTRE BUT LÉGITIME .....</b>	<b>54</b>
Article 132 : Définition du traitement dans tout autre but légitime .....	54
Article 133 : Les conditions de traitement .....	54
Article 134 : La conservation des données .....	54
<b>CHAPITRE II : RÈGLEMENT DES DIFFÉRENDS .....</b>	<b>55</b>
Article 135 : Règlement des différends .....	55
<b>ANNEXE : CHARTE D'ACCÈS AU SYSTÈME D'INFORMATION D'INTERPOL PAR LES ENTITÉS NATIONALES .....</b>	<b>56</b>

# RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

## PRÉAMBULE

L'Assemblée générale de l'Organisation internationale de police criminelle - INTERPOL,

Vu le Statut de l'Organisation, et notamment son article 2, paragraphe 1,

Après consultation de la Commission de contrôle des fichiers d'INTERPOL conformément à l'article 36, paragraphe 2 du Statut,

Considérant qu'il appartient à l'Assemblée générale, conformément à l'article 8(d) du Statut d'arrêter les règles de fonctionnement du Système d'information d'INTERPOL en matière de traitement de données,

A ADOPTÉ LES RÈGLES SUIVANTES :

## **Article 1 : Définitions**

Aux fins du présent Règlement, on entend par :

1. Infractions de droit commun : toute infraction pénale, à l'exception de celles qui entrent dans le champ d'application de l'article 3 du Statut et de celles pour lesquelles un régime spécifique a été défini par l'Assemblée générale.
2. Données : tout élément d'information, quelle que soit sa source, portant sur des faits constitutifs d'infractions de droit commun, les investigations les concernant, la prévention, les poursuites contre son ou ses auteurs et la sanction de ces infractions, la disparition de personnes ou l'identification de cadavres.
3. Données à caractère personnel : toutes données concernant une personne physique identifiée ou susceptible d'être identifiée par des moyens auxquels on peut raisonnablement recourir.
4. Système d'information d'INTERPOL : l'ensemble structuré des moyens matériels et logiciels mis en œuvre par l'Organisation, bases de données, infrastructure de communication, technologies avancées utilisant des capteurs et autres services, permettant le traitement de données par son canal dans le cadre de la coopération policière internationale.
5. Traitement : toute opération ou ensemble d'opérations, appliqué à des données, effectué ou non à l'aide de procédés automatisés, tel que la collecte, l'enregistrement, la consultation, la transmission, l'utilisation, la divulgation ou l'effacement.
6. Source : tout Bureau central national qui traite des données dans le Système d'information d'INTERPOL ou pour le compte de qui des données sont traitées dans ce système et qui en est responsable en dernier ressort, ou toute entité internationale ou toute entité privée dont les données sont traitées dans le Système d'information d'INTERPOL, et qui en est responsable en dernier ressort.
7. Bureau central national : tout organisme désigné par un pays pour assurer les fonctions de liaison prévues à l'article 32 du Statut de l'Organisation.
8. Entité nationale : entité légalement autorisée à exercer une mission de service public qui a été expressément autorisée par le Bureau central national de son pays, par voie d'accord et dans les limites déterminées par ledit Bureau central national, à consulter directement des données traitées dans le Système d'information d'INTERPOL ou à fournir directement des données pour l'une ou plusieurs des finalités de traitement énumérées à l'article 10 du présent Règlement.
9. Entité internationale : toute organisation internationale, intergouvernementale ou non gouvernementale, exerçant une mission d'intérêt public au plan international, qui a conclu un accord avec l'Organisation relatif à l'échange de données et à qui l'Organisation décide de conférer un accès direct ou indirect à une partie du Système d'information d'INTERPOL.
10. Entité privée : toute personne morale de droit privé, telle qu'une entreprise, une société, une association commerciale ou une association à but non lucratif, ne relevant pas de la catégorie des entités internationales, qui a conclu un accord avec l'Organisation relatif à l'échange de données et en particulier au traitement de données dans le Système d'information d'INTERPOL.
11. Demande de coopération internationale : toute démarche effectuée par l'intermédiaire du Système d'information d'INTERPOL par laquelle un Bureau central national, une entité internationale ou le Secrétariat général sollicite l'assistance d'un ou plusieurs Membres de l'Organisation en vue de l'accomplissement d'une action spécifique conforme aux buts et activités de l'Organisation.
12. Alerte internationale : toute démarche effectuée par l'intermédiaire du Système d'information d'INTERPOL par laquelle un Bureau central national, une entité internationale ou le Secrétariat général avise un ou plusieurs Membres de l'Organisation de menaces spécifiques pour la sécurité publique, les personnes ou les biens.
13. Notice : toute demande de coopération internationale ou toute alerte internationale émise par l'Organisation à la requête d'un Bureau central national ou d'une entité internationale, ou à l'initiative du Secrétariat général, et adressée à l'ensemble des Membres de l'Organisation.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

14. Diffusion : toute demande de coopération internationale ou toute alerte internationale émanant d'un Bureau central national ou d'une entité internationale, transmise directement à un ou plusieurs Bureaux centraux nationaux ou à une ou plusieurs entités internationales et enregistrée simultanément dans une base de données de police de l'Organisation.
15. Message : toute demande de coopération internationale, toute alerte internationale ou toutes données qu'un Bureau central national ou qu'une entité internationale dotée de pouvoirs d'enquête et de poursuite en matière pénale choisit de transmettre directement à un ou plusieurs Bureaux centraux nationaux ou à une ou plusieurs entités internationales par l'intermédiaire du Système d'information d'INTERPOL mais qu'il ou elle choisit, sauf indication contraire, de ne pas enregistrer simultanément dans une base de données de police de l'Organisation.
16. Accès direct : introduction et obtention de données dans le Système d'information d'INTERPOL par des personnes expressément autorisées, à l'aide de procédés automatisés et sans assistance du Secrétariat général.
17. Accès indirect : introduction et obtention, avec l'assistance du Secrétariat général, de données dans le Système d'information d'INTERPOL.
18. Données particulièrement sensibles : toute donnée à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ou relative à la santé et à la vie sexuelle ; ou toute donnée biométrique.
19. Interconnexion : toute liaison électronique consistant à relier une partie du Système d'information d'INTERPOL à une partie d'un autre système d'information.
20. Téléchargement : toute opération informatique consistant à exporter des données contenues dans le Système d'information d'INTERPOL dans un autre système d'information.
21. Téléversement : toute opération informatique consistant à importer dans le Système d'information d'INTERPOL des données contenues dans un autre système d'information.
22. Analyse criminelle : toute opération de recherche et de mise en évidence méthodiques de relations entre des données effectuée dans le cadre de la coopération policière internationale.
23. Statut d'une personne : information sur une personne au regard d'un événement justifiant le traitement de données dans le Système d'information d'INTERPOL.
24. Signalement positif : concordance présumée entre des données déjà enregistrées dans le Système d'information d'INTERPOL et d'autres données qui y sont introduites.
25. Technologie avancée utilisant des capteurs : toute technologie facilitant l'identification de personnes et d'objets à travers le traitement automatisé de données et pouvant permettre la prise de décisions semi-automatiques, ce qui nécessite une intervention humaine à des fins de vérification.
26. Grand ensemble de données : ensemble de données structurées ou non structurées, communiquées par une source de données au Secrétariat général, qui ne sont pas vérifiées ni ne relèvent d'une catégorie et qui, en raison de leur volume ou de leur complexité, ne peuvent être évaluées conformément aux dispositions du présent Règlement lors de leur traitement initial par le Secrétariat général.
27. Base de données de police opérationnelles permanentes : base de données de police permanente créée par le Secrétariat général, quelle que soit la technologie de traitement des données utilisée, conformément aux dispositions de l'article 29 du présent Règlement.
28. Enregistrement : insertion de données ou d'autres informations dans une base de données de police ou un fichier d'analyse criminelle, conformément aux conditions d'enregistrement énoncées dans le présent Règlement.
29. Informations accessibles au public : informations accessibles au public qui ne sont pas soumises à des restrictions légales, sont obtenues sans autorisation ni statut juridique particuliers, et qui comprennent, mais sans s'y limiter, les informations provenant de sources d'information ou des médias, de livres ou de revues spécialisées, de documents publiés sur Internet, de documents universitaires, de bases de données commerciales ou de services par abonnement.
30. Données biométriques : toute donnée à caractère personnel relative aux caractéristiques physiques, biologiques, comportementales ou physiologiques telles que les empreintes digitales, les images faciales ou les profils ADN, ayant fait l'objet d'un traitement technique spécifique pour permettre ou confirmer l'identification d'une personne.

# RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

## **Article 2 : But**

Le présent Règlement vise à garantir l'efficacité et la qualité de la coopération internationale entre autorités de police criminelle par le canal d'INTERPOL dans le respect des droits fondamentaux des personnes au sujet desquelles s'exerce cette coopération, conformément à l'article 2 du Statut de l'Organisation et à la Déclaration universelle des droits de l'homme auquel ledit article renvoie.

## **Article 3 : Objet**

Le présent Règlement définit les principes généraux, les responsabilités et les modalités de fonctionnement du Système d'information d'INTERPOL.

## **Article 4 : Champ d'application**

1. Le traitement des données par le canal INTERPOL s'effectue exclusivement dans le cadre du Système d'information d'INTERPOL.
2. Le présent Règlement s'applique à toute opération de traitement des données effectuée dans le Système d'information d'INTERPOL.
3. Nonobstant les dispositions applicables du présent Règlement, l'Assemblée générale peut adopter un régime juridique distinct par lequel les Membres de l'Organisation conviennent de se conformer à un règlement régissant le traitement des données à des fins de coopération judiciaire internationale.

## **TITRE 1 : PRINCIPES GÉNÉRAUX**

### **CHAPITRE I : PRINCIPES RELATIFS À LA COOPÉRATION POLICIÈRE INTERNATIONALE**

## **Article 5 : Respect des principes de gouvernance et responsabilités associées au traitement des données**

1. La coopération policière internationale par le canal INTERPOL s'effectue dans le cadre des règles générales régissant le fonctionnement de l'Organisation, notamment de son Statut.
2. Le traitement de données dans le Système d'information d'INTERPOL s'effectue, en particulier, conformément aux articles 2, 3, 26, 31, 32, 33 et 41 du Statut de l'Organisation.

3. Les Membres de l'Organisation s'efforcent d'échanger le maximum d'informations présentant un intérêt pour la coopération policière internationale dans le respect de la neutralité politique, de l'indépendance et du mandat de l'Organisation, de leurs législations nationales respectives et des conventions internationales auxquelles ils sont parties.
4. Les Bureaux centraux nationaux assument au plan national un rôle central en matière de traitement de données dans le Système d'information d'INTERPOL.
5. La source des données assume l'entièvre responsabilité des données qu'elle traite dans le Système d'information d'INTERPOL, quelle que soit la méthode employée aux fins de ce traitement, ainsi que des conséquences découlant directement de ce traitement, et prend les mesures appropriées pour remédier à tout traitement de données incorrect.
6. INTERPOL assume l'entièvre responsabilité de toute utilisation et/ou de tout stockage de données non autorisé ou incorrect qu'il aurait effectué, ainsi que des conséquences découlant directement d'une telle utilisation et/ou d'un tel stockage non autorisé ou incorrect, et prend les mesures appropriées pour remédier à tout traitement de données incorrect par l'Organisation.
7. Les destinataires des données traitées dans le Système d'information d'INTERPOL assument l'entièvre responsabilité :
  - a) de toute action entreprise au niveau national à partir des données qu'ils ont reçues ;
  - b) de prendre les mesures appropriées pour que les données reçues soient immédiatement mises à jour au niveau national lorsqu'ils ont été informés de quelque modification ou effacement que ce soit.

## **Article 6 : Accès au Système d'information d'INTERPOL**

1. Les Bureaux centraux nationaux disposent, de droit, d'un accès direct au système pour l'exercice de leurs fonctions statutaires. Cet accès comprend :
  - a) l'enregistrement, la mise à jour et l'effacement de données directement dans les bases de données de police de l'Organisation ainsi que la création de liens entre données ;
  - b) la consultation directe des bases de données de police de l'Organisation, sous réserve des conditions particulières déterminées pour chaque base de données ainsi que des restrictions et règles de confidentialité énoncées par leurs sources ;

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

- c) le recours aux notices INTERPOL et aux diffusions permettant la transmission de demandes de coopération et d'alertes internationales ;
  - d) le suivi des signalements positifs ;
  - e) la transmission de messages.
2. L'accès des entités nationales et des entités internationales au Système d'information d'INTERPOL est soumis à autorisation, dans les conditions prévues respectivement aux articles 21 et 27 du présent Règlement.

### **Article 7 : Maîtrise du traitement des données**

- 1. Les Bureaux centraux nationaux et les entités internationales conservent à tout moment la maîtrise du traitement de leurs données, dans le respect du présent Règlement. Tout Bureau central national ou toute entité internationale est libre en particulier de restreindre l'accès ou l'utilisation de ses données dans une base de données de police de l'Organisation, dans les conditions prévues à l'article 58 du présent Règlement.
- 2. Les données traitées dans le Système d'information d'INTERPOL sont celles communiquées par les Bureaux centraux nationaux, les entités nationales et les entités internationales. Peuvent toutefois être traitées dans le système les données qui sont fournies par les entités privées en application de l'article 28 du présent Règlement ou celles qui sont enregistrées par le Secrétariat général en application de l'article 24(2) du présent Règlement.

### **Article 8 : Recours aux notices INTERPOL et aux diffusions**

- 1. La transmission des demandes de coopération et des alertes internationales par le canal INTERPOL s'effectue par voie de notices INTERPOL ou de diffusions.
- 2. Les notices INTERPOL et les diffusions peuvent être utilisées, de droit, par les Bureaux centraux nationaux pour l'exercice de leurs fonctions statutaires. Pour les entités internationales, cette faculté est soumise à autorisation.
- 3. La publication de notices INTERPOL et la transmission de diffusions s'effectuent conformément aux articles 73 et suivants du présent Règlement.
- 4. Les Bureaux centraux nationaux peuvent formuler des demandes de coopération et des alertes internationales par voie de messages, conformément à l'article 9 ci-dessous. Pour les entités internationales dotées de pouvoirs d'enquête et de poursuite en matière pénale, cette faculté est soumise à autorisation.

### **Article 9 : Communication directe par voie de messages**

- 1. Le Système d'information d'INTERPOL permet la communication directe entre Bureaux centraux nationaux par voie de messages.
- 2. Les Bureaux centraux nationaux ont, de droit, la faculté de transmettre des messages pour l'exercice de leurs fonctions statutaires. Pour les entités internationales, cette faculté est soumise à autorisation.
- 3. Le Bureau central national ou l'entité internationale qui procède à la transmission d'un message s'assure préalablement de sa conformité au présent Règlement.
- 4. Le Secrétariat général ne peut procéder à l'enregistrement d'un message dans une base de données de police de l'Organisation sans le consentement du Bureau central national ou de l'entité internationale qui a procédé à la transmission dudit message. Le consentement du Bureau central national ou de l'entité internationale est présumé lorsque le Secrétariat général est l'un des destinataires dudit message.
- 5. Des facilités supplémentaires de communication directe par voie de messages peuvent être mises en place dans le cadre de projets ou d'initiatives spécifiques. Exceptionnellement, la faculté de transmettre ces messages peut être octroyée par un Bureau central national à des personnes expressément autorisées n'appartenant pas au personnel de celui-ci.

## **CHAPITRE II : PRINCIPES RELATIFS AU TRAITEMENT DE L'INFORMATION**

### **Article 10 : Finalités de la coopération policière**

- 1. Le traitement des données dans le Système d'information d'INTERPOL ne peut être effectué que pour une finalité déterminée, explicite et conforme aux buts et activités de l'Organisation.
- 2. Les données sont traitées dans le Système d'information d'INTERPOL pour au moins l'une des finalités suivantes :
  - a) retrouver une personne recherchée en vue de la détenir, de l'arrêter ou de restreindre ses déplacements ;
  - b) localiser une personne ou un objet présentant un intérêt pour la police ;
  - c) fournir ou obtenir des informations relatives à une enquête pénale ou aux antécédents et activités criminels d'une personne ;

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

- d) alerter au sujet d'une personne, d'un événement, d'un objet ou d'un mode opératoire liés à des activités criminelles ;
  - e) identifier une personne ou un corps ;
  - f) réaliser des analyses de police scientifique ;
  - g) organiser des contrôles de sécurité qui sont directement liés à la coopération policière internationale et qui visent à prévenir ou à détecter les infractions ;
  - h) mener des activités de gestion des frontières et des contrôles aux frontières ;
  - i) identifier des menaces, des tendances en matière de criminalité ainsi que des réseaux criminels, y compris en réalisant des analyses criminelles.
3. Les Bureaux centraux nationaux, les entités nationales et les entités internationales sont responsables de la détermination de la finalité de traitement de leurs données et de leur réévaluation régulière, en particulier chaque fois que cette finalité est susceptible d'avoir été atteinte.
4. Le Secrétariat général est tenu de mettre en place les mécanismes et outils destinés à garantir à tout moment le respect de ladite finalité, dans les conditions prévues aux articles 125 à 127 du présent Règlement.
5. Les Bureaux centraux nationaux, les entités nationales et les entités internationales sont tenus de respecter cette finalité lors de l'utilisation des données.
6. Le traitement des données par les Bureaux centraux nationaux, les entités nationales et les entités internationales pour d'autres finalités en matière de coopération policière internationale ou à des fins administratives n'est permis que dans la mesure où il est conforme aux buts et activités de l'Organisation et n'est pas incompatible avec la finalité pour laquelle les données ont été traitées initialement dans le Système d'information d'INTERPOL. Ledit traitement est notifié à la source qui conserve le droit de s'y opposer, dans les conditions prévues à l'article 64 du présent Règlement. Il s'effectue sous la seule responsabilité du Bureau central national, de l'entité nationale ou de l'entité internationale qui choisit de traiter les données pour d'autres finalités que celle pour laquelle les données ont été traitées initialement.
7. Les données peuvent faire l'objet d'un traitement dans tout autre but légitime, distinct de la coopération policière internationale, dans les conditions prévues aux articles 132 et suivants du présent Règlement.

### **Article 11 : Licéité**

1. Le traitement des données dans le Système d'information d'INTERPOL doit être autorisé au regard du droit applicable au Bureau central national, à l'entité nationale et à l'entité internationale et respecter les droits fondamentaux des personnes au sujet desquelles s'exerce la coopération, conformément à l'article 2 du Statut de l'Organisation et à la Déclaration Universelle des Droits de l'Homme auquel ledit article renvoie.
2. Les Bureaux centraux nationaux, les entités nationales et les entités internationales sont chargés d'assurer la licéité de la collecte et de l'introduction dans le Système d'information d'INTERPOL de leurs données.
3. Les Bureaux centraux nationaux, les entités nationales et les entités internationales sont également chargés d'assurer la licéité de la consultation des données introduites dans le Système d'information d'INTERPOL.

### **Article 12 : Qualité**

1. Les données traitées dans le Système d'information d'INTERPOL doivent être exactes, pertinentes, non excessives par rapport aux finalités et à jour, de manière à permettre leur utilisation par les Bureaux centraux nationaux, les entités nationales et les entités internationales.
2. Les Bureaux centraux nationaux, les entités nationales et les entités internationales sont responsables de la qualité de leurs données dans le Système d'information d'INTERPOL.
3. Le Secrétariat général est tenu de mettre en place les mécanismes et outils destinés à garantir à tout moment le respect de ladite qualité.
4. Les Bureaux centraux nationaux, les entités nationales et les entités internationales sont tenus de vérifier la qualité des données préalablement à leur utilisation, dans les conditions prévues à l'article 63 du présent Règlement.

### **Article 13 : Transparence**

1. Le traitement des données dans le Système d'information d'INTERPOL doit garantir à tout moment aux Bureaux centraux nationaux, aux entités nationales et aux entités internationales, le respect de leurs droits de traitement, conformément au présent Règlement.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

2. Le Secrétariat général est responsable de la transparence des processus de traitement des données et du fonctionnement des bases de données de l'Organisation :
- Il sollicite l'avis de la Commission de contrôle des fichiers d'INTERPOL sur les opérations de traitement de données à caractère personnel visées aux articles 27 à 31, 55, 56, 61, 68(4,d), 73(2) et 97(3) du présent Règlement qu'il envisage ;
  - Il informe la Commission de contrôle des fichiers d'INTERPOL des mesures prises en application des articles 51(7), 59, 118 et 125(2,b) du présent Règlement ;
  - Il soumet au Comité exécutif tout projet ou demande relatif au traitement de données dans le Système d'information d'INTERPOL pour lequel son autorisation préalable est requise en vertu des articles 17(5), 22(3), 23, 29, 30, 31, 55(3), 68(8), 97(3) et 131(3) du présent Règlement et joint l'avis de la Commission de contrôle des fichiers d'INTERPOL chaque fois que celui-ci est requis par le présent Règlement. Le Comité exécutif fait rapport à l'Assemblée générale sur les autorisations qu'il a délivrées dans les conditions prévues à l'article 55(6) du présent Règlement ;
  - Il informe le Comité exécutif des mesures prises en application des articles 59, 68(4) et 118 du présent Règlement ;
  - Il tient à jour, dans les conditions prévues à l'article 126 du présent Règlement, les registres suivants :
    - registre des Bureaux centraux nationaux, des entités nationales et des entités internationales à qui un accès est conféré au Système d'information d'INTERPOL ou dont émanent les données traitées dans le système ;
    - registre des bases de données de police de l'Organisation, y compris des fichiers d'analyse ;
    - registre des opérations d'interconnexion ;
    - registre des opérations de téléchargement et de téléversement ;
    - registre des opérations de traitement des données enregistrées dans les bases de données ;
    - registre des outils de gestion des données mis en œuvre par le Secrétariat général ;
    - registre des opérations de comparaison à des fins de vérification.

Ces registres sont accessibles à tout moment par les Bureaux centraux nationaux. Ils sont également accessibles par les entités internationales selon les droits d'accès qui leur sont conférés ainsi que par les entités nationales par l'intermédiaire de leurs Bureaux centraux nationaux.

- Le Secrétariat général tient à jour une liste des durées maximales de conservation telles que définies par le Comité exécutif conformément au présent Règlement, et rend ladite liste publique.

### **Article 14 : Confidentialité**

- La confidentialité des données traitées dans le Système d'information d'INTERPOL doit être déterminée en fonction des risques liés à leur divulgation pour les personnes au sujet desquelles s'exerce la coopération, les sources et l'Organisation. Ne doivent avoir accès aux données que les personnes habilitées à en connaître.
- Les Bureaux centraux nationaux, les entités nationales et les entités internationales sont responsables de l'attribution de niveaux de confidentialité à leurs données dans le Système d'information d'INTERPOL et du respect de la confidentialité des données qu'ils consultent, transmettent ou utilisent à des fins de traitement externe, dans les conditions prévues aux articles 112 et suivants du présent Règlement.
- Le Secrétariat général s'assure que toutes les données sont traitées dans le Système d'information d'INTERPOL selon le niveau de confidentialité que leur a attribué le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à leur traitement.
- Le Secrétariat général prend, dans le respect du présent Règlement, toute mesure nécessaire et appropriée de renforcement de la confidentialité attachée à des données afin de se prémunir contre le risque que leur divulgation pourrait faire courir aux personnes au sujet desquelles s'exerce la coopération, aux sources et à l'Organisation.

### **Article 15 : Sécurité**

- Les données traitées dans le Système d'information d'INTERPOL doivent être protégées contre les risques d'atteinte à leur intégrité et à leur confidentialité et demeurer disponibles pour les Bureaux centraux nationaux, les entités nationales et les entités internationales disposant de l'accès direct au Système d'information d'INTERPOL.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

2. Le Secrétariat général est chargé de mettre en place un système de gestion de la sécurité de l'information. À cette fin et en concertation avec les Bureaux centraux nationaux ou avec leurs représentants au sein des organes consultatifs créés à cet effet, il définit et met à jour régulièrement une politique en matière de sécurité reposant sur des normes acceptées au niveau international et fondée sur l'évaluation du risque encouru.
3. Le Secrétariat général est chargé de mettre en place l'infrastructure de communication et les bases de données destinées à préserver la sécurité des données conformément à la politique de sécurité définie.
4. Le Secrétariat général est chargé de définir les procédures d'autorisation ou d'habilitation de sécurité de son personnel pour chaque niveau de confidentialité des données dans les conditions prévues aux articles 112 et suivants du présent Règlement.
5. Les Bureaux centraux nationaux et les entités internationales sont responsables des accès qu'ils confèrent au Système d'information d'INTERPOL, de la sécurité des installations leur permettant l'accès audit système, du respect des règles de sécurité établies et du maintien d'un niveau de sécurité des données au moins équivalent à celui défini par le Secrétariat général en cas de traitement externe.
6. Le Secrétariat général prend, dans le respect du présent Règlement, toute mesure appropriée afin de préserver la sécurité des données traitées dans le Système d'information d'INTERPOL.

### **Article 16 : Traitement externe à des fins de police**

1. Les données initialement traitées dans le Système d'information d'INTERPOL peuvent être traitées hors du Système d'information d'INTERPOL si ce traitement est nécessaire et effectué à des fins de police. Tout traitement externe doit être effectué dans le respect des principes relatifs au traitement de l'information ci-dessus.
2. Les Bureaux centraux nationaux et les entités internationales sont responsables de la mise en œuvre des modalités de traitement externe, dans les conditions prévues aux articles 114(4) et 116 du présent Règlement.
3. Le Secrétariat général conseille les Bureaux centraux nationaux et les entités internationales concernant la mise en œuvre de ces modalités.

### **Article 17 : Mise en œuvre effective**

1. La mise en œuvre du présent Règlement doit être assurée de manière effective.
2. Les Bureaux centraux nationaux, les entités nationales et les entités internationales sont chargés de définir et de mettre en œuvre les mesures efficaces et appropriées pour garantir la conformité de leurs opérations avec les principes et obligations énoncés dans le présent Règlement, en particulier par la formation de leur personnel.
3. Les Bureaux centraux nationaux sont chargés de définir et de mettre en œuvre les procédures assurant la conformité des opérations de leurs entités nationales avec les principes et obligations énoncés dans le présent Règlement avant de les autoriser à consulter directement des données traitées dans le Système d'information d'INTERPOL ou à fournir directement des données aux fins de traitement dans ledit système.
4. Les Bureaux centraux nationaux sont chargés de procéder à l'évaluation régulière du fonctionnement de chacune de leurs entités nationales au regard du présent Règlement et prennent, dans la limite du présent Règlement, toute mesure corrective nécessaire et appropriée vis-à-vis desdites entités nationales, afin de mettre fin à tout traitement non conforme des données. Ils peuvent prendre toute mesure de précaution nécessaire afin de prendre en compte le risque inhérent à l'utilisation de données manifestement non conforme.
5. Le Secrétariat général est chargé de procéder à l'évaluation régulière du fonctionnement des Bureaux centraux nationaux au regard du présent Règlement. Il prend toute mesure corrective nécessaire et appropriée afin de mettre fin à tout traitement non conforme des données, dans les conditions prévues à l'article 131 du présent Règlement. Toute mesure qui aurait pour effet de suspendre de manière prolongée les droits de traitement d'un Bureau central national est soumise à l'autorisation préalable du Comité exécutif.
6. Le Secrétariat général est chargé de procéder à l'évaluation régulière du fonctionnement des entités internationales au regard du présent Règlement, et adopte toute mesure corrective nécessaire et appropriée afin de mettre fin à tout traitement non conforme des données, dans les conditions prévues à l'article 131 du présent Règlement.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

### **Article 18 : Droits d'accès, de rectification et d'effacement des données**

1. Toute personne ou entité est en droit de saisir directement la Commission de contrôle des fichiers d'INTERPOL d'une demande d'accès à des données la concernant traitées dans le Système d'information d'INTERPOL, et/ou de rectification ou d'effacement de telles données.
2. Ces droits d'accès à des données, et/ou de rectification ou d'effacement de données sont garantis par la Commission de contrôle des fichiers d'INTERPOL et font l'objet d'un règlement distinct. Sauf disposition expresse dudit Règlement, les demandes d'accès et/ou de rectification ou d'effacement de données ne peuvent pas être traitées dans le Système d'information d'INTERPOL.

3. Les Bureaux centraux nationaux sont chargés d'assurer le suivi des demandes de coopération et alertes internationales qu'ils ont transmises à la demande des services de leur pays par voie de notices INTERPOL, de diffusions et de messages.

### **Article 21 : Délivrance des autorisations d'accès direct au plan national**

1. Les Bureaux centraux nationaux sont seuls habilités à autoriser des entités de leur pays à accéder au Système d'information d'INTERPOL et à fixer l'étendue de leurs droits d'accès et de traitement.
2. Préalablement à la délivrance d'autorisations d'accès direct, les Bureaux centraux nationaux doivent s'assurer que toutes les conditions suivantes sont remplies :
  - a) l'entité à laquelle il est envisagé de conférer un accès direct au Système d'information d'INTERPOL est une entité nationale telle que définie à l'article 1(8) du présent Règlement ;
  - b) la nature des activités et des missions de cette entité ne porte pas atteinte aux buts et à la neutralité de l'Organisation ;
  - c) la législation nationale n'interdit pas un tel accès à cette entité ;
  - d) cette entité sera en mesure de respecter le présent Règlement ;
  - e) les droits d'accès et de traitement qu'il est envisagé de conférer sont limités et sont strictement nécessaires et proportionnés à l'exécution des tâches et à l'exercice des fonctions de cette entité.
3. La délivrance par un Bureau central national d'une autorisation d'accès direct au Système d'information d'INTERPOL fait l'objet d'un accord préalable entre ledit Bureau central national et la nouvelle entité nationale. L'accord doit être conforme à la « Charte d'accès au Système d'information d'INTERPOL par les entités nationales » figurant en annexe du présent Règlement.
4. Lorsqu'un Bureau central national délivre une autorisation à une nouvelle entité nationale, il le notifie immédiatement au Secrétariat général ainsi qu'à l'ensemble des Bureaux centraux nationaux et des entités internationales.
5. Les entités nationales traitent leurs données dans le Système d'information d'INTERPOL dans la limite des droits de traitement qui leur sont conférés.

### **TITRE 2 : ACTEURS**

#### **CHAPITRE I : FONCTIONS DES BUREAUX CENTRAUX NATIONAUX**

### **Article 19 : Coordination des flux de données**

1. Les Bureaux centraux nationaux sont chargés de coordonner au plan national le traitement dans le Système d'information d'INTERPOL de données provenant de leur pays.
2. Les Bureaux centraux nationaux sont chargés de fournir aux services de leur pays, dans le respect du présent Règlement, les données traitées dans le Système d'information d'INTERPOL nécessaires à l'accomplissement de leurs missions.

### **Article 20 : Coordination des recherches criminelles**

1. La coordination des questions de recherches criminelles s'effectue auprès des Bureaux centraux nationaux.
2. Les Bureaux centraux nationaux sont chargés de coordonner au plan national le traitement des demandes de coopération et alertes internationales, qui leur sont adressées par voie de notices INTERPOL, de diffusions et de messages. À ce titre, ils sont libres de déterminer les voies les plus appropriées au plan national pour une coopération internationale efficace.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

6. Les Bureaux centraux nationaux communiquent à leurs entités nationales les informations nécessaires à l'exercice de ces droits de traitement.
7. Les Bureaux centraux nationaux sont responsables du traitement des données effectué par les entités nationales qu'ils autorisent à accéder au Système d'information d'INTERPOL.

## CHAPITRE II : FONCTIONS DU SECRÉTARIAT GÉNÉRAL

### Article 22 : Administration du système

1. Le Secrétariat général est chargé de l'administration générale du Système d'information d'INTERPOL.
2. Il conçoit, organise et administre le Système d'information d'INTERPOL et détermine notamment les technologies sur lesquelles il doit reposer. Lors de la mise en œuvre des technologies de traitement des données, le Secrétariat général veille à ce que les exigences du présent Règlement soient intégrées dès la conception et par défaut le plus tôt possible au moyen de mesures techniques et organisationnelles appropriées.
3. Il examine et traite, sous le contrôle du Comité exécutif et dans le respect du présent Règlement, les demandes de téléchargement et d'interconnexion soumises par les Bureaux centraux nationaux, dans les conditions prévues aux articles 55 et 56 du présent Règlement.
4. Il héberge les bases de données de l'Organisation.
5. Il assure la supervision du traitement des données dans le Système d'information d'INTERPOL et veille au respect des conditions de traitement des données dans les bases de données de l'Organisation. Il met en place les outils permettant la gestion des données et des accès au système. Il exerce son contrôle dans le cadre de vérifications d'office ou d'incidents de traitement.
6. Il gère l'infrastructure de communication d'INTERPOL permettant l'échange direct de données par l'intermédiaire du Système d'information d'INTERPOL. Nonobstant toute obligation applicable en vertu du titre 1, chapitre II, et de l'article 22(5) du présent Règlement, lorsque le Secrétariat général n'est pas un destinataire de l'échange ou lorsqu'il n'y a pas accès, son rôle se limite à ce qui suit :
  - a) Il garantit la sécurité des échanges de données, conformément à l'article 15 du présent Règlement ;

- b) Il prend des mesures pour examiner les dispositions du présent Règlement et veiller à leur respect lorsqu'il prend connaissance d'une violation possible de celui-ci ou des dispositions applicables à un projet spécifique, et prend notamment des mesures en application du titre 4, chapitre III, du présent Règlement ;
- c) À l'exception des mesures requises pour exercer son rôle défini au paragraphe 6(b) ci-dessus, le Secrétariat général n'a pas accès au contenu des échanges directs au sein de l'infrastructure de communication d'INTERPOL sans l'autorisation expresse de l'entité concernée.

### Article 23 : Mesures supplémentaires de renforcement de la coopération

1. Le Secrétariat général est habilité à proposer à l'Assemblée générale la conclusion d'accords en matière de traitement des données, et au Comité exécutif la création de bases de données, de notices INTERPOL ou de diffusions, dans les conditions prévues respectivement aux articles 27, 28, 29, 73 et 97 du présent Règlement.
2. Le Secrétariat général peut, dans la limite du présent Règlement, procéder à des tests aux fins d'examen et d'élaboration des propositions ci-dessus.

### Article 24 : Enregistrement des données

1. Le Secrétariat général procède, en conformité avec le présent Règlement, à l'enregistrement, à la mise à jour et à l'effacement des données dans les bases de données de police de l'Organisation :
  - a) pour le compte de sources ne disposant pas d'un accès au Système d'information d'INTERPOL ;
  - b) de sa propre initiative, s'agissant des données constituant des informations accessibles au public ou des données émanant de personnes ou d'entités ayant contacté le Secrétariat général, les Bureaux centraux nationaux, des entités internationales ou des entités privées, dans les conditions prévues à l'article 47 du présent Règlement, ou encore des données résultant d'analyses criminelles produites par le Secrétariat général ;
  - c) à titre exceptionnel, à la demande et pour le compte d'un Bureau central national ou d'une entité nationale ou d'une entité internationale disposant d'un accès direct au Système d'information d'INTERPOL.

2. Le Secrétariat général ne peut procéder à un enregistrement pour le compte de sources ne disposant pas d'un accès au Système d'information d'INTERPOL ou de sa propre initiative que si des procédures de mises à jour et d'effacement des données ont été définies préalablement.

#### **Article 25 : Coordination**

1. Le Secrétariat général facilite la coopération des Bureaux centraux nationaux entre eux. Il sollicite auprès d'eux ou leur transmet, dans le respect du présent Règlement et des restrictions et règles de confidentialité énoncées par la source, toutes données qu'il estime susceptibles de permettre une meilleure coordination de la coopération internationale.
2. Le Secrétariat général peut, si les besoins de la coopération internationale l'exigent, exercer une coordination directe avec des entités nationales, sous réserve de l'autorisation expresse de leurs Bureaux centraux nationaux respectifs.
3. Le Secrétariat général facilite chaque fois que nécessaire la coopération des Bureaux centraux nationaux avec les entités internationales et privées.
4. Afin de permettre une meilleure coordination de la coopération internationale, le Secrétariat général peut publier de sa propre initiative des notices, dans les conditions prévues à l'article 103 du présent Règlement.

#### **Article 26 : Mesures d'urgence**

1. Lorsque les mécanismes de coopération établis par l'Organisation, son indépendance, ou l'exécution de ses engagements sont menacés d'une manière grave et immédiate et que le fonctionnement régulier du Système d'information d'INTERPOL est susceptible d'être interrompu, le Secrétaire Général prend en matière de traitement des données les mesures appropriées exigées par ces circonstances, après consultation officielle du Président de l'Organisation. Il en informe les Bureaux centraux nationaux ainsi que la Commission de contrôle des fichiers. Ces mesures doivent être inspirées par la volonté d'assurer aux Bureaux centraux nationaux, dans les moindres délais, les moyens d'accomplir leurs fonctions statutaires.
2. Lorsque des personnes ou des biens sont menacés d'une manière réelle et imminente et que les données permettant à un Bureau central national, à une entité nationale ou à une entité internationale de prévenir la menace font l'objet de restrictions d'accès à son encontre, le Secrétariat général est autorisé à engager la procédure d'urgence prévue à l'article 59 du présent Règlement.

**CHAPITRE III :**  
**RELATIONS AVEC LES ENTITÉS**  
**INTERNATIONALES ET LES ENTITÉS**  
**PRIVÉES**

#### **Article 27 : Conditions relatives au traitement des données par les entités internationales**

1. Chaque fois qu'elle l'estime souhaitable, compte tenu des buts et objectifs précisés dans le Statut de l'Organisation, l'Organisation peut établir des relations avec des entités internationales afin de collaborer de manière régulière avec elles en matière de traitement des données. L'établissement de relations régulières entre l'Organisation et une entité internationale s'effectue par voie d'accord.
2. Le Secrétariat général sollicite l'avis de la Commission de contrôle des fichiers sur tout projet d'accord dès lors qu'il concerne le traitement de données à caractère personnel.
3. Le Secrétariat général soumet pour approbation à l'Assemblée générale tout projet d'accord. Il fournit à l'appui de sa demande :
  - a) les objectifs de l'accord, ses modalités et implications ;
  - b) le résultat des tests éventuellement conduits par le Secrétariat général ;
  - c) l'avis de la Commission de contrôle des fichiers dès lors que le projet d'accord concerne le traitement de données à caractère personnel ;
  - d) le texte du projet d'accord.
4. Le traitement des données par les entités internationales est soumis aux conditions cumulatives suivantes :
  - a) l'entité internationale est une organisation internationale, intergouvernementale ou non gouvernementale, exerçant une mission d'intérêt public au plan international ;
  - b) ce traitement est strictement limité à la finalité de la collaboration envisagée entre l'entité internationale et l'Organisation ;
  - c) le traitement des données à caractère personnel est strictement limité au besoin d'en connaître de ladite entité ;
  - d) l'entité internationale s'engage dans l'accord à respecter les principes de traitement et les obligations générales incomptant à toute source, tels qu'énoncés dans le présent Règlement ;
  - e) l'Organisation et l'entité internationale ont conclu un accord sur les modalités de traitement des données transmises entre les deux parties.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

5. L'accès direct par les entités internationales à une partie du Système d'information d'INTERPOL est soumis aux conditions supplémentaires suivantes :
  - a) l'entité internationale accepte les dispositions du présent Règlement, et consent à s'y conformer, ainsi qu'aux dispositions spécifiques de l'accord ;
  - b) l'entité internationale accepte toute règle de sécurité et procédure administrative que le Secrétariat général pourrait mettre en place en application du présent Règlement pour permettre l'accès au Système d'information d'INTERPOL et son utilisation, et consent à s'y conformer ;
  - c) l'entité internationale accepte que des contrôles réguliers sur le traitement par l'entité des données transmises par INTERPOL soient effectués à distance ou sur site ;
  - d) l'accès n'est conféré qu'à une seule unité ou département au sein de ladite entité ;
  - e) l'accès ne peut avoir pour effet d'interrompre ou de retarder la transmission des demandes de coopération et des alertes, ou l'accès à ces demandes et alertes, par les Bureaux centraux nationaux ;
  - f) l'entité internationale souhaitant pouvoir transmettre directement par voie de message des données à un ou plusieurs Bureaux centraux nationaux ou à une ou plusieurs entités internationales est dotée de pouvoirs d'enquête et de poursuite en matière pénale ;
  - g) l'entité internationale souhaitant pouvoir demander la publication de notices INTERPOL ou transmettre des diffusions est dotée de pouvoirs d'enquête et/ou de poursuite en matière pénale. L'utilisation du système des notices spéciales par une entité internationale est en revanche examinée au cas par cas.
6. La décision de l'Organisation d'approuver un nouvel accès par une entité internationale au Système d'information d'INTERPOL est notifiée par le Secrétariat général aux Bureaux centraux nationaux et aux entités internationales. L'accès n'est effectif qu'à l'issue d'une procédure garantissant aux autres Bureaux centraux nationaux et aux autres entités internationales la maîtrise des droits de traitement de leurs données conférés à la nouvelle entité, dans les conditions prévues à l'article 109 du présent Règlement.
7. La liste des accords conclus est communiquée chaque année au Comité exécutif, à la Commission de contrôle des fichiers et à l'Assemblée générale.

### Article 28 : Conditions relatives au traitement des données par les entités privées

1. Dans la mesure où cela est utile à l'accomplissement de ses buts, l'Organisation peut établir des relations avec des entités privées souhaitant collaborer avec elle en matière de traitement des données. L'établissement et la conduite de relations entre l'Organisation et une entité privée s'effectue par voie d'accord.
2. Le Secrétariat général sollicite l'avis de la Commission de contrôle des fichiers sur tout projet d'accord dès lors qu'il concerne le traitement de données à caractère personnel.
3. Le Secrétariat général soumet pour approbation à l'Assemblée générale tout projet d'accord. Il fournit à l'appui de sa demande :
  - a) les objectifs de l'accord, ses modalités et implications ;
  - b) le résultat des tests éventuellement conduits par le Secrétariat général ;
  - c) l'avis de la Commission de contrôle des fichiers dès lors que le projet d'accord concerne le traitement de données à caractère personnel ;
  - d) le texte du projet d'accord.
4. Toute coopération avec une entité privée doit :
  - a) respecter le Statut d'INTERPOL et en particulier le principe de souveraineté nationale. Tout Bureau central national qui a enregistré des données dans le Système d'information d'INTERPOL ou pour le compte de qui des données ont été enregistrées dans le système peut s'opposer à la retransmission de ses données à une entité privée ;
  - b) être soumise à des accords, dont la conclusion a préalablement été autorisée par le Comité exécutif puis approuvée par l'Assemblée générale.
5. Une telle coopération ne peut être envisagée que si :
  - a) l'entité privée est une personne morale de droit privé ;
  - b) le traitement est conforme aux buts et aux activités de l'Organisation ;
  - c) la finalité de la coopération est clairement déterminée et correspond à l'une des activités de prévention des infractions de droit commun ;
  - d) elle doit présenter un intérêt pour la coopération policière internationale par rapport à la finalité recherchée ;
  - e) il est envisagé une coopération durable ;

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

- f) le type de données auquel l'accès est rendu possible est identifié de manière précise ;
  - g) les données émanant de l'entité privée sont identifiées comme telles et ne peuvent être confondues avec des données provenant d'autres sources ;
  - h) l'indépendance de l'Organisation dans sa coopération avec l'entité privée est garantie ;
  - i) la coopération avec l'entité privée n'interfère pas avec la transmission des demandes de coopération et des alertes internationales ;
  - j) l'entité privée s'engage dans l'accord à respecter les principes de traitement et les obligations générales incombant à toute source, tels qu'énoncés dans le présent Règlement.
6. Les données fournies aux entités privées doivent être limitées aux données analytiques et ne peuvent pas être à caractère personnel. Néanmoins, à titre exceptionnel, les données fournies aux entités privées peuvent s'étendre, dans le cadre d'un projet spécifique, aux données à caractère personnel (à l'exclusion des données nominatives, sauf si les Bureaux centraux nationaux ou les entités internationales qui ont fourni les données l'autorisent expressément) ou aux données utilisées dans un contexte opérationnel. Dans ce cas, les conditions supplémentaires suivantes doivent être remplies :
- a) les limites de projet doivent être clairement définies ;
  - b) le projet doit faire l'objet d'un accord préalable avec les entités concernées ;
  - c) l'accès à ces données est strictement limité au besoin d'en connaître de ladite entité ;
  - d) l'utilisation des données doit être proportionnelle aux finalités mentionnées à l'article 10(2) du présent Règlement.
7. Les conditions de traitement des données par les entités privées sont fixées dans l'accord conclu entre l'entité privée et l'Organisation.
8. Avant de fournir des données à des entités privées selon les autorisations et conditions fixées par l'accord, le Secrétariat général le informe à la source de ces données. Il ou elle dispose de 45 jours à compter de cette notification pour s'opposer à cette communication.
9. Les modalités de communication de données aux entités privées doivent être déterminées dans l'accord de façon à garantir la sécurité et l'intégrité des données traitées dans le Système d'information d'INTERPOL.
- 10. Le Secrétariat général devra s'assurer que les moyens utilisés par une entité privée pour fournir ou obtenir des données traitées dans le Système d'information d'INTERPOL ne lui permettent d'accéder qu'aux seules données autorisées, conformément à l'accord conclu à cet effet. Il devra veiller à ce que les entités privées ne puissent ni accéder à des données opérationnelles, ni compromettre ou interférer avec des communications de police.
  - 11. En aucun cas, le Système d'information d'INTERPOL ne peut être utilisé pour contourner les contraintes imposées par toute législation nationale en matière de coopération policière avec une entité privée.
  - 12. La liste des accords conclus est communiquée chaque année au Comité exécutif, à la Commission de contrôle des fichiers et à l'Assemblée générale.

## TITRE 3 : MODALITÉS DE TRAITEMENT DES DONNÉES

### CHAPITRE I : BASES DE DONNÉES DE POLICE

#### SECTION 1 : AUTORISATION

##### Article 29 : Crédit d'une base de données

1. Le Secrétariat général soumet au Comité exécutif pour approbation tout projet de création d'une base de données de police.
2. Il fournit à l'appui de sa demande :
  - a) les motifs ayant conduit le Secrétariat général à élaborer ce projet ainsi que les implications financières de celui-ci ;
  - b) la liste des caractéristiques générales de cette base de données, établie en concertation avec les Bureaux centraux nationaux ou avec leurs représentants au sein des organes consultatifs créés à cet effet ;
  - c) le résultat des tests éventuellement conduits par le Secrétariat général ;
  - d) l'avis de la Commission de contrôle des fichiers dès lors que la base contient des données à caractère personnel ou est reliée à de telles données ;

## **RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES**

---

3. Toute création d'une base de données de police est immédiatement notifiée aux Bureaux centraux nationaux. Elle est également notifiée aux entités internationales selon les droits d'accès au Système d'information d'INTERPOL qui leur sont conférés.
- Article 30 : Modification d'une base de données existante**
1. Le Secrétariat général est habilité à procéder à la modification des bases de données de police.
  2. Le Secrétariat général sollicite l'avis de la Commission de contrôle des fichiers sur tout projet de modification d'une base de données ayant pour effet de modifier les caractéristiques générales de celle-ci dès lors que la base contient des données à caractère personnel ou est reliée à de telles données.
  3. Le Secrétariat général soumet au Comité exécutif pour approbation tout projet de modification d'une base de données ayant pour effet de modifier les caractéristiques générales de celle-ci.
  4. Il joint à cet effet :
    - a) les motifs ayant conduit le Secrétariat général à proposer de modifier cette base de données ainsi que les implications financières de la modification ;
    - b) la liste révisée des caractéristiques propres à cette base de données, définie en concertation avec les Bureaux centraux nationaux ou avec leurs représentants au sein des organes consultatifs créés à cet effet ;
    - c) le résultat des tests éventuellement conduits par le Secrétariat général ;
    - d) l'avis de la Commission de contrôle des fichiers dès lors que la base contient des données à caractère personnel ou est reliée à de telles données.
  5. Toute modification portant sur les caractéristiques générales d'une base de données de police est immédiatement notifiée aux Bureaux centraux nationaux. Elle est également notifiée aux entités internationales selon les droits d'accès au Système d'information d'INTERPOL qui leur sont conférés.

2. Le Secrétariat général soumet au Comité exécutif pour approbation tout projet de suppression d'une base de données.
3. Il joint à cet effet :
  - a) les motifs ayant conduit le Secrétariat général à proposer cette suppression ainsi que les implications financières de celle-ci ;
  - b) le rapport soumis par le Secrétariat général à la Commission de contrôle des fichiers et l'avis de celle-ci.
4. Toute suppression d'une base de données de police est immédiatement notifiée aux Bureaux centraux nationaux. Elle est également notifiée aux entités internationales selon les droits d'accès au Système d'information d'INTERPOL qui leur sont conférés.

**Article 32 : Autorisations accordées par le Comité exécutif**

1. Le Comité exécutif fait rapport chaque année à l'Assemblée générale sur les autorisations qu'il a accordées en matière de création, modification ou suppression de bases de données de police de l'Organisation en indiquant notamment leur place dans l'ensemble du Système d'information d'INTERPOL, leur finalité, la nature des données qu'elles accueillent et les droits de traitement attachés à chaque base.
2. Le Comité exécutif fait également rapport à l'Assemblée générale sur la durée maximale de conservation qu'il a fixée pour chaque type de données traitées dans le Système d'information d'INTERPOL, en indiquant les motifs de sa décision.

**Article 33 : Registre des bases de données existantes**

1. Le Secrétariat général tient à jour le registre des bases de données de police de l'Organisation. Le registre précise les caractéristiques générales de chacune d'entre elles.
2. Les Bureaux centraux nationaux peuvent accéder à ce registre à tout moment. Les entités internationales peuvent accéder à une partie de ce registre, selon les droits d'accès au Système d'information d'INTERPOL qui leur sont conférés.

**Article 31 : Suppression d'une base de données existante**

1. Le Secrétariat général fait rapport à la Commission de contrôle sur toute suppression envisagée d'une base de données et du traitement des données contenues dans ladite base.

**SECTION 2 :  
FONCTIONNEMENT**

**Article 34 : Respect du Statut de l'Organisation**

1. Conformément à l'article 5 du présent Règlement, avant tout enregistrement de données dans une base de données de police, le Bureau central national, l'entité nationale ou l'entité internationale s'assure de leur conformité à l'article 2 du Statut de l'Organisation, en particulier qu'il ou elle est autorisé(e) à les enregistrer au regard des lois nationales et des conventions internationales qui lui sont applicables ainsi que des droits fondamentaux des personnes conformément à la Déclaration Universelle des Droits de l'Homme auquel ledit article renvoie.
2. Conformément à l'article 5 du présent Règlement, avant tout enregistrement de données dans une base de données de police, le Bureau central national, l'entité nationale ou l'entité internationale s'assure de leur conformité à l'article 3 du Statut de l'Organisation.
3. Pour déterminer la conformité de données à l'article 3 du Statut de l'Organisation, tous les éléments pertinents sont examinés, notamment :
  - a) la nature de l'infraction, à savoir les chefs d'accusation et les faits concernés ;
  - b) le statut des personnes ;
  - c) l'identité de la source des données ;
  - d) la position exprimée par un autre Bureau central national ou une autre entité internationale ;
  - e) les obligations de droit international ;
  - f) les implications au regard de la neutralité de l'Organisation ;
  - g) le contexte général de l'affaire.
4. Le Secrétariat général pourra élaborer et mettre à la disposition des Bureaux centraux nationaux, des entités nationales et des entités internationales des recueils de pratiques, notamment sur l'application des articles 2 et 3 du Statut de l'Organisation, à la lumière des directives émanant de l'Assemblée générale et des évolutions du droit international.

**Article 35 : Intérêt des données pour la coopération policière internationale**

1. Conformément à l'article 5(3) du présent Règlement, avant tout enregistrement de données dans une base de données de police, le Bureau central national, l'entité nationale ou l'entité internationale s'assure qu'elles présentent un intérêt pour la coopération policière internationale.

2. Le respect de cette condition d'enregistrement est évalué au regard :

- a) des finalités spécifiques à la coopération policière internationale énoncées à l'article 10(2) du présent Règlement, et
- b) du caractère international des données, et en particulier de la mesure dans laquelle les Bureaux centraux nationaux, les entités nationales ou les entités internationales autres que la source seront susceptibles de les utiliser.

**Article 36 : Caractéristiques générales des bases de données**

1. Toute base de données de police est définie au regard des caractéristiques générales suivantes :
  - a) la finalité spécifique de la base de données ;
  - b) la nature des données qu'elle contient, en particulier s'il s'agit de données à caractère personnel ou de données particulièrement sensibles ;
  - c) les sources susceptibles d'alimenter la base de données ;
  - d) les niveaux de confidentialité applicables ;
  - e) le type de restrictions applicable ;
  - f) les mesures de sécurité applicables ;
  - g) les Bureaux centraux nationaux et les entités nationales ou internationales susceptibles de procéder à l'enregistrement des données dans la base de données ;
  - h) les conditions minimales d'enregistrement ;
  - i) les modalités d'enregistrement des données, en particulier tout traitement spécifique effectué sur les données lors de l'enregistrement en raison de leur nature ;
  - j) les modalités de mise à jour des données enregistrées ;
  - k) la durée de conservation des données et les modalités spécifiques de prolongation ou d'effacement ;
  - l) les procédures et mécanismes de vérification de la conformité des données ;
  - m) les Bureaux centraux nationaux et les entités nationales ou internationales susceptibles de consulter la base de données ;
  - n) les modalités de consultation de la base de données, notamment tout type d'accès direct ou toute opération d'interconnexion ou de téléchargement ;
  - o) les modalités d'utilisation des données ;

## **RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES**

---

- p) les procédures à respecter si un signalement positif est généré à partir de données enregistrées dans la base de données ;
  - q) les données pouvant être divulguées au public conformément à l'article 61 du présent Règlement.
2. L'ensemble des caractéristiques générales ci-dessus détermine le régime juridique applicable à chaque base de données de police de l'Organisation.

### **Article 37 : Conditions minimales d'enregistrement dans les bases de données**

1. Des conditions minimales d'enregistrement sont définies pour chaque base de données.
2. Quelle que soit la base de données, l'enregistrement de données relatives à des personnes, objet ou événement doit comporter :
  - a) l'identité de la source des données ;
  - b) la date de l'enregistrement ;
  - c) la finalité spécifique de l'enregistrement ;
  - d) pour toute donnée à caractère personnel, le statut de la personne et les données liant cette personne à un événement ;
  - e) le niveau de confidentialité des données ;
  - f) la durée de conservation des données ;
  - g) les restrictions d'accès ;
  - h) toute donnée complémentaire garantissant la pertinence de l'ensemble des données au regard de la finalité et l'intérêt pour la coopération policière internationale.
3. Ces conditions sont définies par le Secrétariat général en concertation avec les Bureaux centraux nationaux ou avec leurs représentants au sein des organes consultatifs créés à cet effet, et sont communiquées à l'ensemble des Bureaux centraux nationaux. Elles sont également communiquées aux entités internationales selon les droits d'accès qui leur sont conférés.
4. Tout Bureau central national, toute entité nationale ou toute entité internationale veille au respect des conditions minimales d'enregistrement lors de l'enregistrement de données dans une base de données de police.
5. Tout Bureau central national, toute entité nationale ou toute entité internationale conservera toute pièce à l'origine de l'enregistrement des données ou justifiant leur conservation dans la base de données.

### **Article 38 : Conditions supplémentaires d'enregistrement de données relatives à des personnes**

1. Des conditions supplémentaires d'enregistrement de données relatives à des personnes sont mises en œuvre dans les cas suivants :
  - a) données relatives à des personnes décédées ;
  - b) données relatives à des personnes victimes ou témoins ;
  - c) données relatives à des personnes mineures ;
  - d) données particulièrement sensibles.
2. Tout Bureau central national ou toute entité nationale ou toute entité internationale s'assure du respect de ces conditions supplémentaires d'enregistrement lors de l'enregistrement de données dans une base de données de police.

### **Article 39 : Conditions supplémentaires d'enregistrement relatives aux personnes décédées**

1. Les données relatives aux personnes décédées ne peuvent être enregistrées que dans les seuls cas suivants :
  - a) en vue d'identifier la personne ;
  - b) si la personne a joué un rôle dans un fait criminel ou événement traité dans les bases de données de police de l'Organisation et que les données la concernant sont nécessaires à la compréhension dudit fait ou dudit événement ;
  - c) à des fins d'analyse criminelle.
2. Les données sont enregistrées pour le temps strictement nécessaire à l'accomplissement d'une des finalités de traitement ci-dessus.
3. Le statut de ces personnes et la finalité de l'enregistrement sont précisés de telle sorte que les données ne puissent être confondues, de quelque manière que ce soit, avec celles concernant des personnes au sujet desquelles s'exerce la coopération.

### **Article 40 : Conditions supplémentaires d'enregistrement relatives aux personnes victimes ou témoins**

1. Les données relatives aux personnes victimes ou témoins sont enregistrées exclusivement dans le contexte des faits dont les personnes sont victimes ou témoins et ne peuvent être utilisées en relation avec d'autres faits. Le statut de ces personnes et la finalité de l'enregistrement sont précisés de telle sorte que les données ne puissent être confondues, de quelque manière que ce soit, avec celles concernant des personnes suspectées, accusées ou condamnées pour ces mêmes faits.

## **RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES**

---

2. Une mention supplémentaire est apposée précisant qu'aucune mesure de contrainte ne doit être prise à leur encontre.

### **Article 41 : Conditions supplémentaires d'enregistrement relatives aux personnes mineures**

1. Une mention supplémentaire « MINEUR » doit être apposée chaque fois que la personne était mineure au moment des faits qui font l'objet de l'enregistrement. La minorité s'apprécie au regard de la législation nationale du Bureau central national ou de l'entité nationale qui procède à l'enregistrement des données. Pour une entité internationale, elle s'apprécie au regard des règles qui lui sont applicables.
2. Dans ce cas, le Bureau central national, l'entité nationale ou l'entité internationale qui procède à l'enregistrement des données précise les conditions spécifiques éventuelles imposées par la législation qui lui est applicable.

### **Article 42 : Conditions supplémentaires de traitement relatives aux données particulièrement sensibles**

1. Les données particulièrement sensibles ne peuvent être traitées dans le Système d'information d'INTERPOL que si :
  - a) elles sont pertinentes et présentent une valeur criminalistique particulièrement importante pour la poursuite des buts de l'Organisation et des finalités du traitement visées à l'article 10(2) du présent Règlement ;
  - b) elles sont décrites sous une forme objective et ne comportent aucun jugement ou commentaire discriminatoire.
2. Les données biométriques sont considérées comme pertinentes et présentant une valeur criminalistique particulièrement importante lorsqu'elles sont traitées dans le Système d'information d'INTERPOL :
  - a) pour identifier ou confirmer l'identité d'une personne, d'un cadavre, ou les restes humains non identifiés d'une personne ;
  - b) pour éviter les erreurs d'identification d'une personne dans le cadre de la coopération policière internationale ;
  - c) pour établir des liens entre des infractions et des scènes de crime.
3. Lorsqu'elles sont enregistrées dans l'une des bases de données de l'Organisation, les données particulièrement sensibles sont enregistrées de manière à ce que, lors de leur consultation, elles soient identifiées en tant que telles.

4. La retransmission de données particulièrement sensibles est effectuée conformément à l'article 67 du présent Règlement.
5. Les données particulièrement sensibles ne doivent en aucun cas être traitées, sous quelque forme que ce soit, dans un but discriminatoire.

### **Article 43 : Conditions supplémentaires d'enregistrement relatives aux données copiées ou téléversées**

1. Des données d'une base de données de police de l'Organisation ne peuvent être copiées dans une autre base de police de l'Organisation ou dans une partie du Système d'information d'INTERPOL qu'aux conditions cumulatives suivantes :
  - a) lorsque les données sont copiées pour la même finalité, la source des données ne s'y est pas opposée dans un délai de 10 jours ;
  - b) lorsque les données sont copiées pour une autre finalité, la source a consenti au traitement pour cette nouvelle finalité ;
  - c) le fait de copier des données n'est pas susceptible de porter atteinte à l'intégrité et à la confidentialité desdites données ;
  - d) les données sont copiées à l'identique ;
  - e) les données sont mises à jour régulièrement.
2. Le Secrétariat général s'assure du respect de ces conditions supplémentaires d'enregistrement lorsque des données d'une base de données de police de l'Organisation sont copiées dans une autre base de police de l'Organisation.
3. Des données ne peuvent être téléchargées dans le Système d'information d'INTERPOL qu'aux conditions cumulatives suivantes :
  - a) le téléchargement est effectué par un Bureau central national, une entité nationale, une entité internationale ou le Secrétariat général ; il s'effectue conformément aux dispositions du présent Règlement ;
  - b) les données sont copiées à l'identique ;
  - c) le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé au téléchargement des données en assure la mise à jour régulière.

### **Article 43A : Conditions supplémentaires relatives au traitement temporaire de grands ensembles de données**

1. Le Secrétariat général peut traiter temporairement de grands ensembles de données afin de déterminer s'ils présentent un intérêt aux fins de la coopération policière internationale et d'évaluer leur conformité au présent Règlement.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

2. En concertation avec la source des données, ce traitement temporaire peut notamment comprendre la structuration, le formatage, l'évaluation et la catégorisation des données et leur recouplement avec des données déjà traitées dans le Système d'information d'INTERPOL.
  3. Le traitement temporaire satisfait aux conditions suivantes :
    - a) Les données satisfont aux principes généraux applicables définis dans le titre 1 du présent Règlement ;
    - b) Les données sont traitées dans un environnement de traitement protégé au sein du Système d'information d'INTERPOL. Les données sont séparées des autres données opérationnelles ou analytiques, et sont distinguées des données fournies par d'autres sources ;
    - c) La durée de conservation des données dans cet environnement est déterminée par la source, mais elle ne peut dépasser la durée de conservation maximale déterminée par le Comité exécutif ;
    - d) L'accès aux données est limité aux services et aux membres du personnel autorisés du Secrétariat général titulaires d'une autorisation d'accès spécifique ;
    - e) Toutes autres conditions définies par la source des données.
  4. Après avoir procédé à l'évaluation des données, le Secrétariat général communique les résultats de cette évaluation à la source des données et efface les données non conformes dans les meilleurs délais.
  5. La source des données peut traiter les données conformes pour une ou plusieurs des finalités de traitement énumérées à l'article 10 du présent Règlement.
  6. Le Secrétariat général efface ensuite les données restantes dans l'environnement de traitement temporaire et en informe la source des données.
- Article 44 : Statut des personnes**
1. Lors de tout enregistrement de données relatives à une personne au sujet de laquelle s'exerce la coopération policière internationale, le Bureau central national, l'entité nationale ou l'entité internationale qui s'apprête à y procéder est tenu de préciser le statut de cette personne à partir notamment de la liste suivante :
    - a) Condamné : Personne qui, par décision judiciaire, a été reconnue coupable de la commission d'une infraction de droit commun ;
    - b) Accusé : Personne à l'encontre de qui des poursuites pénales ont été engagées pour la commission supposée d'une infraction de droit commun ;
    - c) Suspect : Personne qui est considérée dans le cadre d'une enquête criminelle comme auteur possible d'une infraction mais à l'encontre de qui des poursuites n'ont pour l'heure pas été engagées ;
    - d) Antécédents criminels : Personne connue des services chargés de l'application de la loi en raison d'une condamnation pénale passée ou de faits criminels antérieurs pour lesquels elle n'a pas été mise hors de cause ;
    - e) Témoin : Personne non suspecte susceptible de donner des informations utiles dans le cadre d'une enquête criminelle ou d'une enquête sur une disparition ;
    - f) Victime : Personne à l'encontre de qui une infraction a été commise ;
    - g) Disparu : Personne dont le lieu de séjour est inconnu et ayant été signalée comme disparue ;
    - h) Personne non identifiée : Personne en vie, ayant commis une infraction ou non, et dont on cherche à établir l'identité ;
    - i) Cadavre non identifié : Personne décédée, ayant commis une infraction ou non, et dont on cherche à établir l'identité ;
    - j) Décédé (identifiée) : Personne au sujet de laquelle des données sont conservées dans les bases de données de police d'INTERPOL après confirmation de son décès ;
    - k) Menace potentielle : Personne qui est susceptible de constituer une menace pour la sécurité publique ;
    - l) Objet de sanctions de l'ONU : Personne faisant l'objet de sanctions décidées par le Conseil de sécurité des Nations Unies.
  2. D'autres statuts peuvent être créés par le Secrétariat général en concertation avec les Bureaux centraux nationaux et les entités internationales ou avec leurs représentants au sein des organes consultatifs créés à cet effet.

**Article 45 : Définition des conditions particulières d'utilisation lors de l'enregistrement**

Tout Bureau central national, toute entité nationale ou toute entité internationale qui procède à l'enregistrement de données précise les conditions d'utilisation de ces données une fois introduites dans le Système d'information d'INTERPOL, et en particulier les conditions éventuelles liées à l'utilisation des données à titre de preuve dans un procès pénal.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

### **Article 46 : Mise à jour**

1. Conformément à l'article 12(1) du présent Règlement, le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à l'enregistrement de données est tenu de procéder à leur mise à jour régulière.
2. Lorsque la finalité pour laquelle des données ont été enregistrées est atteinte, ces données ne peuvent être mises à jour ou conservées dans la base de données de police de l'Organisation que si le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à l'enregistrement détermine une nouvelle finalité d'enregistrement et justifie ce changement de finalité.
3. Le Bureau central national, l'entité nationale ou l'entité internationale qui procède à la mise à jour de données s'assure que les conditions d'enregistrement des données sont respectées.
4. Le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à l'enregistrement de données peut par ailleurs à tout moment modifier :
  - a) la durée de conservation des données ;
  - b) leur niveau de confidentialité ;
  - c) les restrictions d'accès aux données ;
  - d) leurs conditions de consultation ;
  - e) leurs conditions d'utilisation.

### **Article 47 : Conditions supplémentaires relatives à l'enregistrement des informations accessibles au public et des informations émanant de personnes ou d'entités**

1. Les conditions supplémentaires ci-après s'appliquent à l'enregistrement des informations accessibles au public et des informations émanant de personnes ou d'entités qui ont contacté le Secrétariat général, les Bureaux centraux nationaux, des entités internationales ou des entités privées :
  - a) L'enregistrement des informations est conforme aux buts et activités de l'Organisation, peut concourir à leur réalisation, et est pertinent aux fins de la coopération policière internationale, telle que définie dans l'article 10(2) du présent Règlement ;
  - b) Les informations sont traitées conformément à l'article 10(2) du présent Règlement, en complément des données figurant dans le Système d'information d'INTERPOL ;

- c) L'origine des informations est clairement indiquée et les informations sont traitées d'une manière permettant de les distinguer clairement des données, telles que définies à l'article 1(2) du présent Règlement, qui sont enregistrées dans le Système d'information d'INTERPOL ;
  - d) Avant leur enregistrement, le Secrétariat général évalue ces informations au regard des articles 11 et 12 du présent Règlement ;
  - e) Conformément aux politiques mises en place par le Secrétariat général et à l'article 50 du présent Règlement, ces informations sont horodatées lors de leur enregistrement, mises à jour ou corrigées s'il y a lieu, puis automatiquement effacées au terme de la durée de conservation maximale définie par le Comité exécutif ;
  - f) Lorsqu'il met ces informations à la disposition des Bureaux centraux nationaux, d'entités nationales, d'entités internationales ou d'entités privées, le Secrétariat général en indique clairement l'origine et communique son évaluation de leur qualité et de leur fiabilité ;
  - g) Avant d'utiliser un rapport ou autre produit du Secrétariat général qui est fondé en tout ou partie sur ces informations, les Bureaux centraux nationaux, entités nationales, entités internationales ou entités privées devraient procéder, dans le respect de leur législation, à une évaluation indépendante de la qualité et de la fiabilité desdites informations ;
  - h) Les informations visées par la présente disposition ne peuvent servir de fondement exclusif à l'application de mesures coercitives par un Bureau central national, une entité nationale ou une entité internationale.
2. La source des informations visées par la présente disposition est :
    - a) le Secrétariat général lorsque :
      - i. les informations accessibles au public sont recueillies par le Secrétariat général ou à son initiative ; ou
      - ii. les informations émanent d'une source (personne ou entité) autre que celles mentionnées à l'article 1(6) du présent Règlement ;
    - b) la source mentionnée à l'article 1(6) du présent Règlement, lorsque les informations émanent de cette source.

**Article 48 : Compléments d'information et correction**

1. Si un Bureau central national, une entité nationale ou une entité internationale autre que celui ou celle qui a procédé à l'enregistrement des données dispose d'éléments pertinents et concrets permettant de considérer que ces données sont incorrectes, il ou elle le fait immédiatement savoir au Bureau central national qui a procédé à l'enregistrement ou pour le compte de qui une entité nationale a enregistré ces données, ou à l'entité internationale qui a procédé à l'enregistrement.
2. Si un Bureau central national, une entité nationale ou une entité internationale autre que celui ou celle qui a procédé à l'enregistrement des données veut les compléter, il ou elle peut adresser ces compléments d'information audit bureau ou à ladite entité internationale.
3. Le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à l'enregistrement est tenu d'examiner sans délai ces informations, et s'il y a lieu de modifier, compléter, rectifier ou effacer immédiatement les données.

**Article 49 : Durée de conservation**

1. Conformément à l'article 10 du présent Règlement, les données ne peuvent être conservées dans les bases de données de police de l'Organisation que le temps nécessaire à l'accomplissement de la finalité pour laquelle elles ont été enregistrées.
2. Les données sont initialement enregistrées pour la durée maximale déterminée par le Comité exécutif pour ce type de données, sous réserve d'une durée de conservation inférieure fixée par la source ou de l'accomplissement de ladite finalité.
3. La durée de conservation s'entend à compter de la date d'enregistrement des données.
4. La suspension d'une demande de coopération ou d'une alerte visée aux articles 81 et 100 du présent Règlement est sans effet sur la durée de conservation des données.

**Article 50 : Évaluation régulière**

1. Aux fins de réévaluation de la finalité du traitement de données et de leur qualité conformément aux articles 10 et 12 du présent Règlement, le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à l'enregistrement des données doit, à l'échéance de la date de conservation de ses données, examiner la nécessité de conserver lesdites données et le cas échéant vérifier que les conditions d'enregistrement sont toujours réunies.

2. Le Secrétariat général sollicite le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à l'enregistrement des données au plus tard six mois avant l'échéance du délai de conservation, pour lui demander d'examiner la nécessité de conserver ces données.
3. Le Secrétariat général précise notamment :
  - a) si les données sont liées à d'autres données provenant de ce même Bureau central national ou de cette même entité ;
  - b) si les données sont traitées dans le cadre d'un projet d'analyse ;
  - c) si les données concernent une forme de criminalité grave ou un domaine de criminalité particulier pour lequel l'Assemblée générale a défini une politique de conservation spécifique mise en œuvre par le Secrétariat général.
4. Si le Bureau central national, l'entité nationale ou l'entité internationale conclut à la conservation des données, il ou elle précise la raison de cette conservation. L'enregistrement des données est prolongé pour une nouvelle période n'excédant pas la durée maximale de conservation, sous réserve d'une durée de conservation inférieure fixée par la source ou de l'accomplissement de ladite finalité.
5. Si le Bureau central national, l'entité nationale ou l'entité internationale conclut que la finalité pour laquelle les données ont été enregistrées est atteinte mais que la conservation des données dans les bases de données de police de l'Organisation continue de présenter un intérêt pour la coopération policière au niveau international, en particulier s'il correspond à l'un des trois cas de figure énoncés ci-dessus, il ou elle détermine une nouvelle finalité d'enregistrement et justifie ce changement de finalité. L'enregistrement des données est prolongé pour une nouvelle période n'excédant pas la durée maximale de conservation correspondant à cette nouvelle finalité, sous réserve d'une durée de conservation inférieure fixée par la source ou de l'accomplissement de ladite finalité.
6. Le Bureau central national, l'entité nationale ou l'entité internationale qui conclut à la conservation des données s'assure que les conditions d'enregistrement des données sont toujours respectées.
7. Le Comité exécutif est habilité, pour une base de données de police de l'Organisation déterminée, à déroger aux modalités ci-dessus de réévaluation des données, à la condition que cette dérogation soit nécessaire.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

### **Article 51 : Effacement de données**

1. Si le Bureau central national, l'entité nationale ou l'entité internationale décide de ne pas conserver des données au titre de l'une des finalités énoncées à l'article 10, ces données sont effacées automatiquement pour la finalité à laquelle elles étaient destinées.
2. Les données sont également toutes effacées automatiquement, à l'échéance de la date de conservation, si le Bureau central national, l'entité nationale ou l'entité internationale ne s'est pas prononcé sur la nécessité de maintenir les données pour la finalité à laquelle elles sont destinées.
3. Lorsque la finalité pour laquelle des données ont été enregistrées est atteinte, le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à l'enregistrement procède à leur effacement des bases de données de police, sauf à ce qu'il ou elle choisisse de déterminer une nouvelle finalité d'enregistrement et justifie ce changement de finalité.
4. Lorsque le Secrétariat général dispose d'éléments pertinents et concrets permettant de considérer que la finalité pour laquelle des données ont été enregistrées est atteinte ou que les données ne remplissent plus les conditions minimales d'enregistrement, il sollicite le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à l'enregistrement des données dans les meilleurs délais pour lui demander d'examiner la nécessité de conserver ces données.
5. Lorsque le Secrétariat général efface des données enregistrées par un Bureau central national, une entité nationale, une entité internationale et concernant une personne faisant l'objet d'une demande de coopération internationale ou d'une alerte, il en informe le Bureau central national ou l'entité internationale qui a procédé à l'enregistrement de ces données, et explique les raisons ayant motivé l'opération.
6. Lorsque des données sont effacées d'une base de données de l'Organisation, toute copie de ces données contenues dans le Système d'information d'INTERPOL est également effacée, sauf si les données sont conservées pour une autre finalité énoncée à l'article 10, et sous réserve du consentement préalable du Bureau central national, de l'entité nationale ou de l'entité internationale qui a procédé à l'enregistrement initial desdites données.

7. Lorsque l'effacement de données s'avère impossible en raison du coût et du volume de travail ainsi occasionnés, le Secrétariat général prend toute mesure appropriée afin de rendre les données inexploitables, d'empêcher l'accès auxdites données et leur utilisation aux fins d'une enquête criminelle, ou de mentionner clairement que les données doivent désormais être considérées comme inexistantes. Il en informe la Commission de contrôle des fichiers.

### **Article 52 : Conservation temporaire des antécédents criminels**

1. Le Bureau central national, l'entité nationale ou l'entité internationale qui procède au retrait d'une alerte ou d'une demande de coopération internationale à l'encontre d'une personne condamnée, accusée, suspectée ou constituant une menace potentielle peut choisir de conserver temporairement les données relatives à cette personne en vue d'informer de ses antécédents criminels.
2. La conservation temporaire des antécédents criminels est interdite s'agissant de personnes condamnées, accusées, suspectées ou constituant une menace qui ont été mises hors de cause pour les faits ayant justifié l'enregistrement initial des données les concernant.
3. Le Bureau central national, l'entité nationale ou l'entité internationale qui conserve des données exclusivement à des fins d'information s'assure que cette conservation est licite au regard du droit national. L'entité internationale, s'assure que cette conservation est licite au regard des règles qui lui sont applicables.
4. La finalité de cet enregistrement ainsi que le statut de la personne concernée sont précisés, respectivement, conformément aux articles 10 et 44(1) du présent Règlement, de telle sorte que les données ne puissent être confondues avec celles concernant des personnes faisant l'objet d'alertes ou de demandes de coopération internationale. Il est gardé trace du statut attribué initialement à la personne concernée.
5. Ces données peuvent être conservées pour une durée n'excédant pas la durée maximale déterminée par le Comité exécutif à compter du moment où le Bureau central national, l'entité nationale ou l'entité internationale indique que la finalité initiale est atteinte, sous réserve d'une durée de conservation inférieure fixée par la source. À l'expiration de la durée de conservation, les données sont automatiquement détruites, sauf si le Bureau central national, l'entité nationale ou l'entité internationale décide de conserver des données à des fins d'orientation conformément à l'article 53 ci-dessous.

### **Article 53 : Conservation des données à des fins d'orientation**

1. Le Bureau central national ou l'entité qui procède à l'effacement de données relatives à une personne soupçonnée, accusée ou condamnée pour des faits criminels indique s'il souhaite conserver les données permettant de rediriger vers lui toute demande ultérieure d'un autre Bureau central national ou d'une autre entité relative à cette personne.
2. Le Secrétariat général ne peut conserver, à des fins d'orientation, des données qu'il efface des bases de données de police, sauf consentement exprès du Bureau central national ou de l'entité qui a procédé à leur enregistrement.
3. Les seules données pouvant être conservées à des fins d'orientation sont : le nom du Bureau central national ou de l'entité qui a procédé à leur enregistrement, la référence de l'enregistrement, le nom et le prénom de la personne, le numéro de son document d'identité et la nature dudit document, sa date et son lieu de naissance, ainsi que ses empreintes digitales et son profil d'ADN.
4. Ces données peuvent être conservées pour une durée maximale déterminée par le Comité exécutif, sauf si une durée de conservation plus courte est fixée par la source.

### **SECTION 3 : CONSULTATION**

#### **Article 54 : Accès direct**

1. Conformément à l'article 6 du présent Règlement, une base de données de police de l'Organisation peut être consultable directement par les Bureaux centraux nationaux, sous réserve des restrictions et règles de confidentialité énoncées par la source. Elle peut également être consultable directement par les entités nationales et les entités internationales, sous réserve desdites restrictions et règles de confidentialité et selon les droits d'accès qui leur sont conférés.
2. Le type de données directement consultables est précisé conformément à l'article 36(1,n) dans la liste des caractéristiques générales de cette base de données.

### **Article 55 : Interconnexion**

1. Toute opération d'interconnexion doit répondre aux conditions cumulatives suivantes :
  - a) la finalité, la nature et l'étendue de l'interconnexion sont déterminées, explicites et conformes aux buts et activités de l'Organisation ;
  - b) l'interconnexion présente un intérêt pour la coopération policière internationale ;
  - c) le système d'information à interconnecter offre un niveau de sécurité au moins équivalent à celui du Système d'information d'INTERPOL ;
  - d) l'interconnexion permet le respect des conditions de traitement fixées par les sources des données contenues dans le Système d'information d'INTERPOL et dans le système d'information à interconnecter ;
  - e) l'interconnexion permet la notification immédiate, au Bureau central national, à l'entité nationale ou à l'entité internationale qui a introduit des données dans le Système d'information d'INTERPOL ainsi qu'au Secrétariat général, de tout élément issu des données interconnectées susceptible de présenter un intérêt pour la coopération policière au niveau international.
2. Toute demande d'interconnexion émanant d'une entité nationale doit être transmise par l'intermédiaire de son Bureau central national.
3. Le Secrétariat général soumet au Comité exécutif pour approbation toute demande d'interconnexion. Il fournit :
  - a) la copie de la demande d'interconnexion reçue, précisant notamment le responsable de l'interconnexion au sein du Bureau central national, de l'entité nationale ou de l'entité internationale ;
  - b) l'évaluation de la demande par le Secrétariat général ainsi que les implications financières de celle-ci pour l'Organisation ;
  - c) le résultat des tests éventuellement conduits par le Secrétariat général ;
  - d) l'avis de la Commission de contrôle des fichiers dès lors que la base contient ou est reliée à des données à caractère personnel.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

4. Lorsque le Comité exécutif autorise l'interconnexion, le Secrétariat général informe au préalable les sources des données enregistrées dans la base de données à interconnecter. Le Secrétariat précise l'ensemble des conditions de l'interconnexion.
5. Le Secrétariat général tient à jour le registre des opérations d'interconnexion. Le registre précise les conditions de chacune d'entre elles. Ce registre est accessible à tout moment par les Bureaux centraux nationaux. Il est également accessible par les entités internationales selon les droits d'accès qui leur sont conférés.
6. Le Comité exécutif fait rapport chaque année à l'Assemblée générale des autorisations qu'il a accordées en matière d'opérations d'interconnexion.

### **Article 56 : Téléchargement à des fins de coopération policière internationale**

1. Toute opération de téléchargement doit répondre aux conditions cumulatives suivantes :
  - a) la finalité du téléchargement est déterminée, explicite et conforme aux buts et activités de l'Organisation ;
  - b) la demande présente un intérêt pour la coopération policière internationale ;
  - c) une opération d'interconnexion n'est pas réalisable en raison de son coût et des caractéristiques fonctionnelles ou techniques du système d'information à interconnecter ;
  - d) le système d'information du Bureau central national, de l'entité nationale ou de l'entité internationale offre un niveau de sécurité au moins équivalent à celui du Système d'information d'INTERPOL ;
  - e) les conditions de traitement et d'utilisation des données téléchargées fixées par les sources sont strictement respectées ;
  - f) le téléchargement est effectué pour une durée déterminée n'excédant pas six mois ;
  - g) les données téléchargées sont mises à jour au moins une fois par semaine, y compris lorsque la mise à jour suppose l'effacement de données ;
  - h) les données téléchargées ne sont pas recopiées au sein du système d'information dans lequel elles sont téléchargées ;
  - i) les données téléchargées sont systématiquement effacées lorsque la finalité pour laquelle elles ont été téléchargées est atteinte, et au plus tard à l'issue de la période de six mois ci-dessus ;

- j) le Bureau central national, l'entité nationale ou l'entité internationale qui procède au téléchargement notifie immédiatement au Bureau central national, à l'entité nationale ou à l'entité internationale qui a introduit des données dans le Système d'information d'INTERPOL ainsi qu'au Secrétariat général tout élément issu des données téléchargées susceptible de présenter un intérêt pour la coopération policière au niveau international.
2. Toute demande de téléchargement émanant d'une entité nationale doit être transmise par l'intermédiaire de son Bureau central national.
3. Le Secrétariat général est habilité à autoriser une opération de téléchargement sous réserve :
  - a) du respect des conditions ci-dessus, et
  - b) d'assurances écrites données par le Bureau central national ou l'entité internationale qui a demandé à procéder à une opération de téléchargement selon lesquelles il ou elle respectera lesdites conditions, la finalité du téléchargement, sa nature et son étendue, et
  - c) de la désignation d'un responsable de l'opération de téléchargement au sein du Bureau central national, de l'entité nationale ou de l'entité internationale.
4. Si, pour des raisons techniques ou autres, le Secrétariat général n'est pas en mesure de respecter une ou plusieurs conditions de traitement associée à des données à télécharger, il ne doit pas autoriser le téléchargement desdites données.
5. Le Secrétariat général notifie aux Bureaux centraux nationaux et aux entités internationales toute opération de téléchargement qu'il a autorisée. Il précise l'ensemble des conditions du téléchargement, en particulier les caractéristiques du système d'information du Bureau central national, de l'entité nationale ou de l'entité internationale qu'il a autorisé à procéder au téléchargement. À compter de la notification du Secrétariat général, un Bureau central national ou une entité internationale dispose de 15 jours pour s'opposer à toute possibilité de traitement par ledit Bureau central national ou ladite entité des données qu'il ou elle a introduites dans le Système d'information d'INTERPOL. Au terme du délai prescrit, le Secrétariat général est habilité à procéder au téléchargement, sous réserve des données pour lesquelles des oppositions lui auront été signifiées.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

6. Le Secrétariat général informe le Comité exécutif de l'autorisation de téléchargement qu'il a délivrée. Il fournit à cet effet :
  - a) l'évaluation de la demande par le Secrétariat général ainsi que les implications financières de celle-ci pour l'Organisation ;
  - b) les caractéristiques du système d'information du Bureau central national, de l'entité nationale ou de l'entité internationale dans lequel les données ont été téléchargées ;
  - c) une copie des assurances écrites données par le Bureau central national ou l'entité internationale qui a demandé à procéder à une opération de téléchargement ;
  - d) l'avis de la Commission de contrôle des fichiers dès lors que l'opération de téléchargement contenait des données à caractère personnel ou était reliée à de telles données.
7. Le Secrétariat général est chargé de contrôler le respect des conditions de téléchargement au cours de la période pendant laquelle le téléchargement est autorisé. Il prend toute mesure nécessaire et appropriée afin de procéder à ce contrôle.
8. Le Secrétariat général tient à jour le registre des opérations de téléchargement. Le registre précise les conditions de chacune d'entre elles. Ce registre est accessible à tout moment par les Bureaux centraux nationaux. Il est également accessible par les entités internationales selon les droits d'accès qui leur sont conférés.

### **Article 57 : Accès indirect**

1. Lorsqu'une base de données de police a pour caractéristique de ne pas être consultable directement ou qu'une entité internationale ne dispose que d'un accès indirect à une base de données, le Secrétariat général détermine les modalités de consultation de ladite base de données et en informe les Bureaux centraux nationaux. Il en informe également les entités internationales selon les droits d'accès qui leur sont conférés.
2. Lorsqu'une base de données de police a pour caractéristique d'être consultable directement, le Secrétariat général peut faire droit à une demande d'accès indirect à des données contenues dans ladite base de données dans les cas suivants :
  - a) l'entité internationale ne dispose pas de droits d'accès direct, ou
  - b) l'accès direct est temporairement inopérant, ou

- c) la demande est spécifique ou complexe et les données ne peuvent être obtenues par voie de consultation directe.
3. Toute demande d'accès indirect émanant d'une entité nationale doit être transmise par l'intermédiaire de son Bureau central national.
4. Lorsqu'il examine une demande d'accès indirect, le Secrétariat général s'assure que :
  - a) la demande émane d'un Bureau central national, d'une entité internationale ou d'une entité privée ;
  - b) lorsque la demande émane d'une entité internationale ou d'une entité privée, elle correspond à la finalité pour laquelle l'accès au Système d'information d'INTERPOL a été octroyé ;
  - c) la demande est claire et motivée ;
  - d) le Bureau central national ou l'entité internationale qui a procédé à l'enregistrement des données susceptibles de correspondre à la demande n'a pas défini de restrictions d'accès à l'intention du Bureau central national, de l'entité internationale ou de l'entité privée qui a formulé ladite demande.

### **Article 58 : Restrictions d'accès**

1. Conformément à l'article 7(1) du présent Règlement, tout Bureau central national ou toute entité internationale peut définir à tout moment, à l'encontre d'autres Bureaux centraux nationaux, d'autres entités internationales ou d'entités privées, des restrictions générales d'accès aux données qu'il ou elle a enregistrées dans une base de données de police. Les restrictions d'accès générales définies par un Bureau central national s'appliquent aux données enregistrées par les entités nationales qu'il a autorisées.
2. Tout Bureau central national ou toute entité internationale peut définir à tout moment, à l'encontre d'autres Bureaux centraux nationaux, d'autres entités internationales ou d'entités privées, des restrictions d'accès supplémentaires pour des données enregistrées liées à une personne, un objet ou un événement.
3. Les Bureaux centraux nationaux et les entités internationales ne peuvent définir de restrictions d'accès à l'encontre des seules entités nationales d'autres Bureaux centraux nationaux. Toute restriction d'accès définie à l'encontre d'un Bureau central national s'applique à l'ensemble des entités nationales qu'il a autorisées.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

4. Les restrictions d'accès à des données s'appliquent quel que soit le mode de consultation de la base de données de police.
5. Lorsqu'un Bureau central national, une entité nationale ou une entité internationale consulte une base de données et qu'il ou elle n'a pas accès aux données susceptibles de correspondre à sa recherche, le Secrétariat général peut transmettre la demande au Bureau central national ou à l'entité internationale qui a défini une restriction d'accès à son encontre.
6. Les messages dont le Bureau central national ou l'entité internationale a autorisé l'enregistrement dans une base de données de police de l'Organisation sont réputés restreints à leurs destinataires initiaux, sauf indication contraire dudit bureau ou de ladite entité.
7. Les restrictions d'accès ne peuvent être levées par le Secrétariat général qu'en cas d'urgence, selon la procédure définie à cet effet, ou lorsque les données sont devenues publiques.
8. Les restrictions d'accès sont des données confidentielles traitées conformément à l'article 112 du présent Règlement.

### **Article 59 : Divulgation de données faisant l'objet de restrictions**

La divulgation de données faisant l'objet de restrictions ne peut être effectuée que dans les cas d'urgence prévus à l'article 26(2) du présent Règlement et selon la procédure suivante :

- a) Le Secrétariat général notifie au Bureau central national, à l'entité nationale ou à l'entité internationale qui a procédé à l'enregistrement desdites données que les conditions fixées à l'article 26(2) du présent Règlement sont réunies, et lui fixe un délai, proportionné à la menace, pour s'opposer à la levée des restrictions ;
- b) Toute demande de levée de restrictions adressée à une entité nationale doit être transmise par l'intermédiaire de son Bureau central national ;
- c) À l'expiration du délai fixé par le Secrétariat général et sauf opposition expresse du Bureau central national, de l'entité nationale ou de l'entité internationale qui a procédé à l'enregistrement des données faisant l'objet de restrictions et liées à la menace, les restrictions sont réputées levées ;

- d) Le Secrétariat général informe dans les plus brefs délais le Comité exécutif ainsi que la Commission de contrôle des fichiers de la mise en œuvre de cette procédure d'urgence.

### **Article 60 : Accès par des tiers**

1. Le Secrétariat général peut traiter des demandes d'accès présentées par des organisations internationales ou des personnes morales de droit privé avec lesquelles l'Organisation envisage d'établir des relations afin de collaborer avec elles en matière de traitement des données.
2. Lorsqu'une demande d'accès à des données contenues dans une base de données de police est présentée par ces tiers, le Secrétariat général ne peut transmettre les données qu'avec l'autorisation préalable expresse de la source des données.

### **Article 61 : Divulgation de données au public**

1. Le Secrétariat général sollicite l'avis de la Commission de contrôle des fichiers sur toute politique de divulgation au public de données traitées dans le Système d'information d'INTERPOL qu'il décide d'adopter conformément aux conditions énoncées au paragraphe 2 ci-dessous, dès lors qu'elle concerne le traitement de données à caractère personnel.
2. Les données traitées dans le Système d'information d'INTERPOL ne peuvent être divulguées au public qu'aux conditions cumulatives suivantes :
  - a) la divulgation est effectuée pour l'une au moins des finalités suivantes :
    - i. pour alerter le public ;
    - ii. pour solliciter l'aide du public ;
    - iii. pour toute autre finalité destinée à promouvoir la coopération policière internationale ;
  - b) la source des données a au préalable autorisé la divulgation des données, notamment le type de données pouvant être divulguées, leur mode de divulgation, les destinataires potentiels de cette divulgation ainsi que, le cas échéant, toute condition spécifique relative à cette divulgation ;
  - c) la divulgation est conforme aux buts et activités de l'Organisation et est effectuée dans le respect des droits fondamentaux des personnes au sujet desquelles s'exerce la coopération policière internationale ;

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

- d) la divulgation n'est pas de nature à porter atteinte aux intérêts de l'Organisation ou de ses Membres ;
  - e) la divulgation ne porte pas sur l'auteur d'une infraction qui, au moment des faits criminels considérés, était considéré comme mineur en vertu de la législation applicable du pays du Bureau central national ou de l'entité internationale qui a introduit les données dans le système, sauf si ce Bureau ou cette entité et le Secrétariat général estiment qu'une telle divulgation est essentielle pour la coopération policière internationale, et si la divulgation en question est conforme aux principes applicables de la législation nationale et du droit international.
3. Dans le cas où une notice ou les données qu'elle contient sont divulguées par un Bureau central national, une entité nationale ou une entité internationale autre que la source des données, les deux conditions suivantes doivent être remplies en sus des conditions énumérées au paragraphe 2 ci-dessus :
- a) le Secrétariat général a au préalable autorisé ladite divulgation ;
  - b) les données contenues dans la notice sont copiées à l'identique et mises à jour régulièrement afin qu'elles demeurent exactes.

## SECTION 4 : UTILISATION

### Article 62 : Conditions d'utilisation

Tout Bureau central national, toute entité nationale et toute entité internationale qui s'apprêtent à utiliser des données traitées dans le Système d'information d'INTERPOL sont tenus de vérifier :

- a) leur exactitude et leur pertinence ;
- b) la finalité pour laquelle ils s'apprêtent à les utiliser ;
- c) toute condition particulière d'utilisation ;
- d) en cas de retransmission vers un autre Bureau central national ou une autre entité internationale, les restrictions d'accès à ces données existant à leur encontre.

### Article 63 : Vérification de l'exactitude et de la pertinence des données

1. Tout Bureau central national, toute entité nationale et toute entité internationale qui s'apprêtent à utiliser des données traitées dans le Système d'information d'INTERPOL aux fins de l'application de mesures coercitives, telles que la détention, l'arrestation ou la restriction des

déplacements, s'assurent que ces données sont toujours exactes et pertinentes. Sans préjudice de ce qui précède, toute mesure autorisée par la législation nationale et les traités internationaux applicables peut être prise avant ou pendant la vérification des données.

2. Un Bureau central national procède à cette vérification directement auprès du Bureau central national qui a procédé à l'enregistrement des données. Si les données ont été enregistrées par une entité nationale, il procède à la vérification auprès du Bureau central national de cette entité nationale. Si les données ont été enregistrées par une entité internationale, il procède à la vérification auprès du Secrétariat général.
3. Une entité nationale procède à cette vérification par l'intermédiaire de son Bureau central national.
4. Une entité internationale procède à cette vérification auprès du Bureau central national ou de l'entité internationale exclusivement par l'intermédiaire du Secrétariat général, sauf si des droits d'accès lui ont été conférés.

### Article 64 : Utilisation de données pour une finalité de police criminelle autre que la finalité initiale ou à une fin administrative

1. Conformément à l'article 10(6) du présent Règlement, tout Bureau central national, toute entité nationale et toute entité internationale qui s'apprêtent à utiliser des données pour une finalité de police criminelle autre que la finalité spécifique à la coopération policière internationale pour laquelle les données ont été enregistrées initialement dans les bases de données de police de l'Organisation, ou à une fin administrative indiquée par la source des données en vertu du paragraphe 2 ci-après ou, en l'absence d'une telle indication, prévue par le droit applicable à l'entité qui envisage d'utiliser les données, s'assurent que cette finalité et cette utilisation :
  - a) sont conformes aux buts et activités de l'Organisation ;
  - b) ne sont pas incompatibles avec la finalité initiale ;
  - c) sont licites au regard du droit qui lui est applicable.
2. Chaque source des données est en droit d'indiquer les finalités, autres que celles énumérées à l'article 10(2) du présent Règlement, qui sont considérées comme des fins administratives au regard de sa législation applicable.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

3. Les Bureaux centraux nationaux ou les entités qui envisagent d'utiliser des données selon ce qui est prévu au paragraphe 1 ci-dessus notifient au préalable la source des données :
  - a) Un Bureau central national notifie directement le Bureau central national qui a procédé à leur enregistrement. Si les données ont été enregistrées par une entité nationale, il notifie le Bureau central national de cette entité nationale. Si les données ont été enregistrées par une entité internationale, il notifie le Secrétariat général ;
  - b) Une entité nationale notifie le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à l'enregistrement des données par l'intermédiaire de son Bureau central national ;
  - c) Une entité internationale notifie le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à l'enregistrement des données par l'intermédiaire du Secrétariat général, sauf s'il s'agit d'une entité internationale dotée de pouvoirs d'enquête et de poursuite en matière pénale qui a été autorisée, conformément à l'article 27(5,f) du présent Règlement, à transmettre directement des données par voie de message.
4. À compter de la notification, la source dispose de 10 jours pour s'opposer à l'utilisation des données pour la finalité envisagée, ou pour demander des informations ou un délai supplémentaires pour répondre à la demande relative à cette utilisation. Ce délai peut être réduit par le Secrétariat général en cas d'urgence.

### Article 65 : Utilisation à des fins administratives [supprimé]

### Article 66 : Conditions particulières d'utilisation

1. Conformément à l'article 45 du présent Règlement, le Secrétariat général met en évidence, lors de la consultation de toutes données, les conditions particulières d'utilisation précisées lors de l'enregistrement de celles-ci par un Bureau central national, une entité nationale ou une entité internationale, en particulier les conditions éventuelles liées à l'utilisation des données à titre de preuve dans un procès pénal.
2. Tout Bureau central national, toute entité nationale ou toute entité internationale qui s'apprête à utiliser des données enregistrées dans une base de données de police respecte les conditions d'utilisation particulières fixées par le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à leur enregistrement.

3. Le Secrétariat général s'assure que tout Bureau central national, toute entité nationale ou toute entité internationale qui consulte les données connaît ces conditions d'utilisation particulières, afin qu'il ou elle puisse prendre les mesures qui s'imposent pour les respecter.

### Article 67 : Retransmission des données

1. En amont de la retransmission de données contenues dans les bases de données de police de l'Organisation ou reçues par message à un autre Bureau central national ou à une autre entité internationale, un Bureau central national ou une entité internationale doit vérifier auprès du Secrétariat général ou du Bureau central national, de l'entité nationale ou de l'entité internationale ayant enregistré ces données ou les ayant transmises par message, que lesdites données ne font pas l'objet de restrictions :
  - a) Un Bureau central national procède à cette vérification directement auprès du Bureau central national ayant enregistré ou transmis les données, ou, si les données ont été enregistrées ou transmises par une entité nationale, il procède à la vérification auprès du Bureau central national de cette entité nationale. Si les données ont été enregistrées ou transmises par une entité internationale, il procède à la vérification auprès du Secrétariat général ;
  - b) Une entité internationale procède à cette vérification auprès du Bureau central national, de l'entité nationale ou de l'entité internationale exclusivement par l'intermédiaire du Secrétariat général, sauf s'il s'agit d'une entité internationale dotée de pouvoirs d'enquête et de poursuite en matière pénale qui a été autorisée, conformément à l'article 27(5,f) du présent Règlement, à transmettre directement des données par voie de message.
2. En amont de la retransmission de données particulièrement sensibles contenues dans les bases de données de police de l'Organisation ou dans un message reçu, un Bureau central national, une entité internationale ou le Secrétariat général doit s'assurer que les données à transmettre sont pertinentes, présentent une valeur criminalistique particulièrement importante pour la poursuite des buts de l'Organisation et sont strictement nécessaires aux finalités du traitement visées à l'article 10(2) du présent Règlement.
3. Lors de la retransmission de données, le Bureau central national ou l'entité internationale qui y procède ainsi que le Secrétariat général en cas de demande d'accès indirect, doit indiquer :
  - a) leur source ;

- b) les conditions d'utilisation spécifiques énoncées par celle-ci ;
  - c) leur niveau de confidentialité ;
  - d) leur date d'enregistrement et leur durée de conservation dans les bases de police ;
  - e) le statut de la personne et le type d'action à entreprendre envers elle, en cas de données à caractère personnel ;
  - f) toute modalité de traitement spécifique des données.
4. Il ou elle transmet à la source des données, si nécessaire ou si la source le requiert, une copie de la transmission.
5. Conformément à l'article 58(6) du présent Règlement, le Secrétariat général ne peut retransmettre un message dont il est destinataire à un Bureau central national ou à une entité internationale qui ne l'est pas sans le consentement préalable du Bureau central national ou de l'entité internationale qui a procédé à sa transmission initiale.
- SECTION 5 :  
RÈGLES SPÉCIFIQUES RELATIVES AUX  
FICHIERS D'ANALYSE CRIMINELLE**
- Article 68 : Fichiers d'analyse**
- 1. Les fichiers d'analyse sont des bases de données temporaires créées à des fins d'analyse criminelle, conformément à une liste de caractéristiques générales établie sur la base de l'article 36(1) du présent Règlement et en concertation avec les Bureaux centraux nationaux, les entités nationales et les entités internationales susceptibles d'être impliqués dans le projet d'analyse criminelle concerné.
  - 2. Les principes de traitement et conditions d'enregistrement de données dans les bases de données de l'Organisation fixées par le présent Règlement sont applicables aux fichiers d'analyse, sous réserve des dispositions ci-dessous.
  - 3. Les fichiers d'analyse sont créés par le Secrétariat général, pour une durée initiale n'excédant pas cinq ans.
  - 4. Le Secrétariat général informe le Comité exécutif de tout projet d'analyse criminelle portant création d'un fichier d'analyse, et lui fournit :
    - a) les motifs ayant conduit le Secrétariat général à élaborer ce projet ainsi que les implications financières de celui-ci ;
- b) la liste des Bureaux centraux nationaux, des entités nationales et des entités internationales susceptibles d'être impliqués dans le projet ;
  - c) la liste des caractéristiques générales du fichier d'analyse constituant son cadre juridique ;
  - d) l'avis de la Commission de contrôle des fichiers dès lors que le fichier d'analyse contient des données à caractère personnel ou est relié à de telles données.
5. Le Comité exécutif peut refuser ou annuler la création d'un fichier d'analyse s'il considère qu'il n'est pas satisfait aux exigences du présent Règlement.
6. La création d'un fichier d'analyse ainsi que sa finalité et le régime juridique applicable sont immédiatement notifiés aux Bureaux centraux nationaux et aux entités internationales susceptibles d'être impliqués dans le projet. La participation ultérieure d'un Bureau central national, d'une entité nationale ou d'une entité internationale au projet d'analyse criminelle est soumise à l'accord de tous les Bureaux centraux nationaux et entités internationales qui participent déjà au projet.
7. Les Bureaux centraux nationaux sont chargés de faire les notifications nécessaires à leurs entités nationales respectives.
8. Le Secrétariat général soumet au Comité exécutif pour approbation tout projet de prolongation d'un fichier d'analyse, pour une durée n'excédant pas cinq ans.

**Article 69 : Utilisation des fichiers d'analyse**

- 1. L'accès aux fichiers d'analyse est limité à des services ou à des membres du personnel autorisés du Secrétariat général participant à l'analyse criminelle et titulaires d'une autorisation d'accès spécifique.
- 2. Le Secrétariat général autorise, lorsque cela est nécessaire, des membres du personnel des Bureaux centraux nationaux, des entités nationales et des entités internationales participant au projet et impliqués dans l'analyse criminelle à accéder à un fichier d'analyse donné et à fixer l'étendue de leurs droits d'accès et de traitement. Des droits d'accès et de traitement sont octroyés aux membres du personnel des entités nationales en concertation avec les Bureaux centraux nationaux concernés.
- 3. Les fichiers d'analyse peuvent être reliés ou non aux bases de données de police de l'Organisation, suivant la finalité des fichiers en question et les conditions de sécurité et de confidentialité requises.

4. Les données enregistrées dans un fichier d'analyse peuvent être copiées dans une base de données de l'Organisation, ou inversement, les données enregistrées dans une base de données de l'Organisation peuvent être copiées dans un fichier d'analyse, si les données remplissent les conditions minimales d'enregistrement propres à ladite base, et sous réserve du consentement exprès du Bureau central national, de l'entité nationale ou de l'entité internationale qui a fourni les données.
5. Si les données ou les autres éléments d'information enregistrés dans un fichier d'analyse sont susceptibles de permettre la mise à jour d'une ou plusieurs bases de données de l'Organisation, ou inversement, si les données enregistrées dans d'autres bases de données sont susceptibles de permettre la mise à jour d'un ou plusieurs fichiers d'analyse, le Secrétariat général doit prendre toute mesure appropriée à cette fin.

**Article 70 : Conditions supplémentaires d'enregistrement de données à des fins d'analyse criminelle**

1. Peuvent être enregistrés dans des fichiers d'analyse les données visées à l'article 1(2) du présent Règlement et d'autres éléments d'information, y compris des informations accessibles au public, dans la mesure où ces éléments seraient nécessaires à l'analyse criminelle.
2. Les données et autres éléments d'information enregistrés dans des fichiers d'analyse sont conservés pour une durée maximale déterminée par le Comité exécutif sauf si une durée de conservation plus courte est fixée par la source, à moins que le fichier d'analyse criminelle qui les contient ne soit fermé avant.
3. Si des données sont enregistrées à la fois dans un fichier d'analyse et dans une base de données de police de l'Organisation, les finalités des enregistrements sont précisées de telle sorte que les données ne puissent être confondues.
4. Lors de tout enregistrement dans un fichier d'analyse de données ou d'autres éléments d'information relatifs à une personne au sujet de laquelle s'exerce la coopération policière internationale, le statut de cette personne est précisé notamment à partir de la liste suivante, qui est applicable uniquement dans le cadre de l'analyse criminelle :
  - a) Statuts visés à l'article 44(1) du présent Règlement ;

- b) Autres statuts ci-dessous, créés en application de l'article 44(2) du présent Règlement :
  - i. Associé : personne qui a des contacts sporadiques ou réguliers avec une personne présentant un intérêt au regard d'une enquête criminelle et/ou à l'encontre de qui des poursuites pénales ont été engagées ;
  - ii. Personne d'intérêt : personne pouvant fournir des informations sur une infraction de droit commun.

**Article 71 : Rapports d'analyse criminelle**

1. Les rapports d'analyse criminelle produits dans le cadre des fichiers d'analyse doivent :
  - a) distinguer clairement les données obtenues par le Secrétariat général des conclusions qu'il en a tirées ;
  - b) indiquer la source des données citées, le statut des personnes mentionnées et la date à laquelle l'analyse a été réalisée ;
  - c) préciser qu'avant tout usage de ces rapports et des données et autres éléments d'information qu'ils contiennent, il convient de vérifier, auprès du Secrétariat général et des sources des données, les droits et restrictions qui y sont attachés ;
  - d) préciser lorsque des informations, ou les conclusions que le Secrétariat général en a tirées, sont fondées en tout ou partie sur des informations accessibles au public, et indiquer l'horodatage et l'origine de ces informations.
2. Les rapports d'analyse criminelle sont divulgués aux Bureaux centraux nationaux, aux entités nationales et aux entités internationales participant au projet d'analyse criminelle concerné. Les rapports d'analyse criminelle peuvent être divulgués à d'autres Bureaux centraux nationaux, entités nationales et entités internationales, sous réserve de l'autorisation du Secrétariat général et d'éventuelles restrictions d'accès définies par les sources des données contenues dans les rapports. La divulgation des rapports doit respecter le niveau de confidentialité attribué au fichier d'analyse par le Secrétariat général, ainsi que toute autre mesure de sécurité applicable.
3. Les rapports d'analyse criminelle peuvent être conservés pour une durée maximale déterminée par le Comité exécutif après l'achèvement du projet d'analyse concerné, à condition qu'ils soient utilisés de manière pertinente et conforme aux règles de traitement spécifiées dans le présent Règlement.

**Article 72 : Achèvement des projets d'analyse criminelle**

1. Lorsqu'un projet d'analyse criminelle est achevé :
  - a) les fichiers d'analyse concernés ainsi que les données et les autres éléments d'information qui y sont enregistrés doivent être détruits ;
  - b) le rapport d'analyse criminelle peut être conservé à condition d'empêcher toute utilisation non pertinente ou contraire aux règles de traitement spécifiées dans le présent Règlement.
2. La divulgation du rapport d'analyse criminelle ou de données qui le composent doit respecter les éventuelles restrictions attachées par leurs sources aux données qu'il contient, ainsi que toute autre mesure de sécurité ou de confidentialité qui lui serait attachée.

**CHAPITRE II :**  
**NOTICES ET DIFFUSIONS**

**SECTION 1 :**  
**DISPOSITIONS COMMUNES AUX NOTICES**

**Article 73 : Système des notices INTERPOL**

1. Le système des notices INTERPOL est constitué d'un ensemble de notices publiées pour une finalité spécifique et identifiables par un code couleur, et de notices spéciales publiées dans le cadre d'une coopération spécifique ne relevant pas des catégories de notices précédentes.
2. Une catégorie de notices ou de notices spéciales ne peut être créée qu'après l'approbation de l'Assemblée générale, qui aura préalablement obtenu l'avis de la Commission de contrôle des fichiers dès lors que la notice contient ou est reliée à des données à caractère personnel.
3. Des conditions de publication sont définies pour chaque catégorie de notices ou de notices spéciales. Ces conditions sont au moins équivalentes aux conditions générales d'enregistrement exigées pour ces données dans les bases de données de l'Organisation.

4. Les conditions de publication de chaque catégorie de notices sont définies ci-après. Les conditions de publication de chaque catégorie de notices spéciales sont définies par voie d'accord.

**Article 74 : Rôle du Secrétariat général**

1. Le Secrétariat général est responsable de la publication, au nom de l'Organisation, des notices INTERPOL.
2. En particulier, il est chargé :
  - a) de vérifier la conformité de toute demande de notice au présent Règlement et de procéder à la publication dans les meilleurs délais de toute demande de notice qu'il juge conforme ;
  - b) d'enregistrer simultanément toute notice publiée dans une base de données de l'Organisation afin qu'elle soit directement consultable par les Bureaux centraux nationaux, les entités nationales et les entités internationales selon les droits qui leur sont conférés ;
  - c) de procéder à la traduction de toute notice dans les langues de travail de l'Organisation d'après les directives arrêtées par l'Assemblée générale ;
  - d) d'assister les Bureaux centraux nationaux et les entités internationales en cas de signalement positif ;
  - e) de veiller à ce que toute notice publiée demeure conforme à ses conditions de publication et fasse l'objet d'une évaluation régulière par le Bureau central national ou l'entité internationale à la demande de qui elle a été publiée. À cette fin, il procède régulièrement à un réexamen des notices publiées et consulte les Bureaux centraux nationaux et les entités internationales à l'origine de la demande et les autres Bureaux centraux nationaux.

**Article 75 : Structure des notices INTERPOL**

1. Le Secrétariat général, en concertation avec les Bureaux centraux nationaux ou avec leurs représentants au sein des organes consultatifs créés à cet effet, définit et modifie, s'il y a lieu, la structure de chaque catégorie de notice, sous réserve de respecter ses conditions de publication, ainsi que toutes autres directives ou décisions émanant de l'Assemblée générale ou du Comité exécutif.
2. Sans préjudice des principes énoncés au titre 1 du présent Règlement, la définition de la structure d'une catégorie de notices spéciales s'effectue par voie d'accord entre l'entité internationale et l'Organisation.

## **RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES**

---

3. Une notice peut contenir des données provenant de différentes sources aux conditions cumulatives suivantes :
  - a) les sources ont consenti à ce traitement ;
  - b) ce traitement présente pour le Bureau central national ou l'entité internationale à l'origine de la demande un intérêt concret au regard de cette demande de coopération ou de cette alerte ;
  - c) les données sont clairement identifiées comme provenant de sources différentes ;
  - d) ce traitement ne génère pas de coûts supplémentaires importants.

### **Article 76 : Demande de publication de notice**

1. Les demandes de notice sont transmises dans au moins une des langues de travail de l'Organisation par un Bureau central national ou une entité internationale.
2. Avant de demander la publication d'une notice, le Bureau central national ou l'entité internationale s'assure :
  - a) de la qualité et de la licéité des données qu'il ou elle fournit à l'appui de sa demande ;
  - b) des conditions de publication attachées à sa demande ;
  - c) de l'intérêt des données pour la coopération policière internationale ;
  - d) de la conformité de sa demande à la réglementation d'INTERPOL, en particulier aux articles 2(1) et 3 du Statut, ainsi qu'aux obligations qui s'imposent à lui ou à elle au regard du droit international.

### **Article 77 : Examen de la demande par le Secrétariat général**

1. Toute demande de notice fait l'objet d'un examen de conformité au présent Règlement par le Secrétariat général.
2. Le Secrétariat général ne peut procéder à la publication d'une notice au nom de l'Organisation si :
  - a) les données fournies ne répondent pas aux conditions de publication des notices ;
  - b) la publication de ladite notice ne présente pas dans le cas d'espèce un intérêt pour la coopération policière internationale. Cet intérêt est évalué au regard de la possibilité que la demande puisse être traitée par l'ensemble des Membres de l'Organisation ;

- c) la publication de ladite notice est susceptible de porter atteinte aux intérêts de l'Organisation ou de ses Membres.
3. Pendant la durée de leur examen par le Secrétariat général, les demandes de notices sont enregistrées à titre temporaire dans une base de données de l'Organisation. Une mention supplémentaire doit être apposée de manière à ce que, lors de leur consultation, elles soient identifiées en tant que telles et ne puissent être confondues avec des notices publiées.

### **Article 78 : Demandes incomplètes ou ne répondant pas aux conditions de publication de notices**

1. Lorsqu'une demande est incomplète, le Bureau central national ou l'entité internationale à l'origine de la demande fournit, dans les meilleurs délais et après consultation du Secrétariat général, toutes les données supplémentaires nécessaires à la publication d'une notice.
2. Le Secrétariat général propose au Bureau central national ou à l'entité internationale à l'origine de la demande, chaque fois que cela est possible, la publication d'autres notices lorsque les données fournies sont insuffisantes pour permettre la publication de ladite notice mais correspondent aux finalités et conditions de publication d'une autre notice.
3. Le Secrétariat général propose au Bureau central national ou à l'entité internationale à l'origine de la demande, chaque fois que cela est possible, la transmission par celui-ci ou celle-ci d'une diffusion lorsque la demande ne s'adresse pas à l'ensemble des Membres de l'Organisation ou que les données fournies sont insuffisantes pour permettre la publication d'une notice mais correspondent à la finalité et aux conditions de transmission et d'enregistrement d'une diffusion.

### **Article 79 : Publication des notices**

1. Les notices sont publiées par le Secrétariat général à l'intention de l'ensemble des Bureaux centraux nationaux selon les modalités suivantes :
  - a) Toute publication de notice est notifiée aux Bureaux centraux nationaux le jour de sa publication ;
  - b) Toute notice publiée est directement consultable dans une base de données de police de l'Organisation par les Bureaux centraux nationaux, sous réserve des mesures conservatoires visées à l'article 129 du présent Règlement.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

2. Les notices sont également consultables par :
  - a) les entités nationales, selon les autorisations d'accès conférées par leurs Bureaux centraux nationaux respectifs ;
  - b) les entités internationales, lorsque l'accord conclu avec l'Organisation le prévoit expressément.
3. En dérogation à l'article 58 du présent Règlement, tout Bureau central national ou toute entité internationale qui présente une demande de notice consent à ce que les données qu'il ou elle fournit ne fassent l'objet d'aucune restriction d'accès à l'encontre d'aucun Bureau central national et d'aucune entité nationale que celui-ci a autorisé à consulter des notices. Il ou elle conserve la possibilité de définir des restrictions d'accès aux données qu'il ou elle fournit à l'encontre des entités internationales qui ne sont pas dotées de pouvoirs d'enquête et de poursuite en matière pénale.

### **Article 80 : Mise en œuvre des notices**

1. Les Bureaux centraux nationaux transmettent :
  - a) à toutes les autorités compétentes de leur pays, dans les meilleurs délais et conformément à leur législation nationale, toutes les données contenues dans les notices qu'ils reçoivent, ainsi que les mises à jour concernant ces notices ;
  - b) au Bureau central national et à l'entité internationale à l'origine de la demande ainsi qu'au Secrétariat général toutes les données dont ils disposent relativement à la personne ou à l'objet pour lequel ladite notice a été publiée, en particulier chaque fois que ces données sont de nature à permettre que la finalité de la notice soit atteinte. Une entité nationale transmet ces données par l'intermédiaire de son Bureau central national ;
  - c) au Secrétariat général tout élément susceptible de faire naître un doute quant à la conformité d'une notice au présent Règlement.
2. Le Bureau central national ou l'entité internationale à l'origine de la notice veille à ce que :
  - a) les données qu'il ou elle a fournies dans la notice et sur lesquelles cette notice se fonde demeurent exactes et pertinentes ;

- b) il ou elle transmette au Secrétariat général toute donnée ayant pour effet de modifier le contenu de la notice publiée, et évalue si les modifications imposent le retrait de ladite notice.

### **Article 81 : Suspension, retrait ou annulation d'une notice**

1. Le Bureau central national ou l'entité internationale à l'origine d'une notice peut suspendre sa demande de coopération ou son alerte pour une période n'excédant pas six mois. Il ou elle indique les raisons de cette suspension au Secrétariat général qui procède à la suspension de la notice.
2. Le Bureau central national ou l'entité internationale à l'origine d'une notice est tenu de retirer sa demande de coopération ou son alerte et de demander au Secrétariat général de procéder immédiatement à l'annulation de la notice dès lors que :
  - a) cette demande ou cette alerte a atteint sa finalité, ou
  - b) cette demande ou cette alerte est liée à une ou plusieurs autres demandes ou alertes qui ont atteint leur finalité et sans lesquelles elle ne peut être maintenue, ou
  - c) il ou elle ne souhaite plus la maintenir, ou
  - d) la notice ne remplit plus les conditions de publication d'une notice.
3. Le Secrétariat général procède à l'annulation d'une notice chaque fois que :
  - a) la demande de coopération ou l'alerte à l'origine de la publication de la notice a atteint sa finalité et cette information a été confirmée par le Bureau central national ou l'entité internationale à l'origine de la notice, ou
  - b) cette demande ou cette alerte est liée à une ou plusieurs autres demandes ou alertes qui ont atteint leur finalité et sans lesquelles elle ne peut être maintenue, ou
  - c) la notice ne remplit plus les conditions de publication d'une notice, ou
  - d) le Bureau central national ou l'entité internationale à l'origine de la demande de notice a reçu des données permettant de réaliser l'action requise mais n'a pris aucune mesure à cette fin et, après avoir été consulté, n'a pas donné de raisons satisfaisantes quant à son inaction.

**SECTION 2 :  
DISPOSITIONS PARTICULIÈRES AUX  
NOTICES ROUGES**

**Article 82 : But des notices rouges**

Les notices rouges sont publiées à la demande d'un Bureau central national ou d'une entité internationale dotée de pouvoirs d'enquête et de poursuite en matière pénale pour demander la localisation d'une personne recherchée et sa détention, son arrestation ou la restriction de ses déplacements aux fins de son extradition, de sa remise ou d'une action similaire conforme au droit.

**Article 83 : Conditions particulières applicables à la publication des notices rouges**

1. Critères minimaux

- a) Les notices rouges ne peuvent être publiées que si les conditions cumulatives suivantes sont réunies :
- i. L'infraction concernée est une infraction de droit commun d'une particulière gravité.

Les catégories d'infractions suivantes ne peuvent donner lieu à la publication de notices rouges :

- infractions suscitant dans plusieurs pays des controverses liées au fait qu'elles ont trait à des normes comportementales ou culturelles ;
- infractions liées à des questions d'ordre familial ou privé ;
- infractions résultant d'une violation de lois ou de réglementations de nature administrative ou découlant de différends d'ordre privé, sauf si l'activité criminelle a pour but de faciliter la commission d'une infraction grave ou si l'on soupçonne qu'elle a des liens avec la criminalité organisée.

Le Secrétariat général tiendra à jour une liste non exhaustive d'infractions relevant des catégories susmentionnées, et la communiquera aux Bureaux centraux nationaux et aux entités internationales.

ii. Seuil de sanction défini :

- dans le cas où la personne est recherchée en vue de poursuites pénales, l'acte reproché constitue une infraction punissable d'une peine privative de liberté dont le maximum ne doit pas être inférieur à deux ans ou d'une peine plus lourde ;

- dans le cas où la personne est recherchée en vue de l'exécution d'une condamnation pénale, la peine infligée est au minimum de six mois de prison, et/ou le reliquat de peine est au minimum de six mois.

iii. La demande présente un intérêt pour la coopération policière internationale.

- b) Le Secrétariat général peut décider de publier une notice rouge bien que les critères i. et/ou ii. ci-dessus ne soient pas remplis si, après avoir consulté le B.C.N. ou l'entité internationale autorisée à l'origine de la demande, il considère que la publication de la notice rouge demandée revêtirait une importance particulière pour la coopération policière internationale.
- c) Infractions multiples : Si la demande porte sur plusieurs infractions, la notice rouge peut être publiée pour toutes les infractions entrant dans le champ de la réglementation d'INTERPOL, à condition qu'au moins une des infractions remplisse les critères ci-dessus.

2. Données minimales

a) Éléments d'identification :

Une notice rouge ne peut être publiée que lorsque suffisamment d'éléments d'identification ont été fournis. Seront considérés comme suffisants au minimum l'une des deux combinaisons d'éléments d'identification suivante :

- i. Nom de famille, prénom, sexe, date de naissance (au moins l'année), et l'un des éléments d'identification suivants :
  - signalement, ou
  - profil d'ADN, ou
  - empreintes digitales, ou
  - données figurant dans des documents d'identité (par exemple, passeport ou carte nationale d'identité) ;

ii. Photographie de bonne qualité avec quelques renseignements complémentaires (par exemple un alias, le nom de l'un ou des deux parents, un complément de signalement, un profil d'ADN, des empreintes digitales, etc.).

b) Éléments juridiques :

Une notice rouge ne peut être publiée que lorsque suffisamment d'éléments juridiques ont été fournis. Seront considérés comme suffisants au minimum les éléments juridiques suivants :

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

- i. Exposé des faits, qui doit donner une description concise et claire des activités criminelles de la personne recherchée, incluant la date et le lieu de l'activité criminelle présumée, et
- ii. Qualification de l'infraction ou des infractions, et
- iii. Références des dispositions de la loi pénale réprimant l'infraction (lorsque cela est possible et sous réserve des dispositions de la législation nationale applicable ou des règles de fonctionnement de l'entité internationale, le Bureau central national ou l'entité internationale à l'origine de la demande de notice rouge communique le texte de la ou des dispositions pénales applicables), et
- iv. Peine maximale encourue, peine infligée ou reliquat de peine, et
- v. Référence d'un mandat d'arrêt en cours de validité ou d'une décision de justice ayant le même effet (lorsque cela est possible et sous réserve des dispositions de la législation nationale applicable ou des règles de fonctionnement de l'entité internationale autorisée, le B.C.N. ou l'entité internationale autorisée à l'origine de la demande fournit une copie du mandat d'arrêt ou de la décision de justice).

### **Article 84 : Garanties fournies par le Bureau central national ou l'entité internationale à l'origine de la notice**

Le Bureau central national ou l'entité internationale à l'origine de la notice s'assure que :

- a) L'autorité émettrice du mandat d'arrêt ou de la décision de justice a qualité pour le faire ;
- b) La publication de la notice rouge a été demandée en concertation avec les autorités compétentes en matière d'extradition, et que des assurances ont été données que l'extradition sera demandée lorsque la personne aura été arrêtée, conformément à la législation nationale et/ou aux traités bilatéraux et conventions multilatérales applicables ;
- c) Lorsque le mandat d'arrêt n'a pas été délivré par une autorité judiciaire, la législation du pays à l'origine de la demande ou les règles de fonctionnement de l'entité internationale prévoient un mécanisme de recours devant une autorité judiciaire.

### **Article 85 : Communication de documents susceptibles de faciliter les procédures d'extradition ou de remise par le Bureau central national ou l'entité internationale à l'origine de la notice**

Lorsque cela lui semble utile et approprié, le Bureau central national ou l'entité internationale à l'origine de la notice fournit au Secrétariat général les documents supplémentaires susceptibles de faciliter les procédures d'extradition ou de remise. Le Secrétariat général pourrait faire office de dépositaire de ces documents et les communiquer sur demande aux pays concernés.

### **Article 86 : Examen juridique par le Secrétariat général**

Le Secrétariat général procède à un examen juridique de toutes les demandes de notices rouges préalablement à leur publication, afin de s'assurer de leur conformité au Statut et à la réglementation d'INTERPOL et, en particulier, aux articles 2 et 3 du Statut.

### **Article 87 : Mesures à prendre en cas de localisation de la personne recherchée**

Les mesures suivantes sont prises si une personne faisant l'objet d'une notice rouge est localisée :

- a) Le pays où la personne recherchée a été localisée :
  - i. informe immédiatement le Bureau central national ou l'entité internationale à l'origine de la notice et le Secrétariat général du fait que la personne recherchée a été localisée – sous réserve des restrictions découlant de sa législation nationale et des traités internationaux applicables ;
  - ii. prend toute autre mesure autorisée par sa législation nationale et les traités internationaux applicables telle que procéder à l'arrestation provisoire de la personne recherchée ou bien surveiller ou restreindre ses déplacements.
- b) Le Bureau central national ou l'entité internationale à l'origine de la notice agit immédiatement une fois informé que la personne recherchée a été localisée dans un autre pays et en particulier, veille à la transmission rapide, à la demande du pays dans lequel la personne a été localisée ou du Secrétariat général et dans les délais fixés pour ce cas précis, des données et des pièces justificatives.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

- c) Le Secrétariat général apporte son aide aux Bureaux centraux nationaux et aux entités internationales concernés, notamment en facilitant la transmission des documents liés à la procédure d'arrestation provisoire ou d'extradition, conformément à la législation nationale et aux traités internationaux applicables.

### SECTION 3 : DISPOSITIONS PARTICULIÈRES AUX AUTRES NOTICES

#### Article 88 : Notices bleues

1. Les notices bleues sont publiées pour :
  - a) obtenir des renseignements sur une personne présentant un intérêt au regard d'une enquête criminelle, et/ou
  - b) localiser une personne présentant un intérêt au regard d'une enquête criminelle, et/ou
  - c) identifier une personne présentant un intérêt au regard d'une enquête criminelle.
2. Une notice bleue ne peut être publiée qu'aux conditions suivantes :
  - a) la personne faisant l'objet de la demande est une personne condamnée, accusée, suspectée, témoin ou victime ;
  - b) des renseignements complémentaires sur ses éventuels antécédents judiciaires, sur le lieu où elle se trouve, sur son identité ou sur tout autre aspect utile à l'enquête criminelle sont demandés ;
  - c) suffisamment de données relatives à l'enquête criminelle ou à la personne sont fournies pour que la coopération sollicitée soit efficace.
3. Une notice bleue ne peut être publiée que si elle comporte des éléments d'identification suffisants. Par éléments suffisants, on entend au moins :
  - a) Si la personne est identifiée :
    - i. soit le nom de famille, le prénom, le sexe et la date de naissance (au moins l'année) complétés par la description physique de la personne, le profil d'ADN, les empreintes digitales ou les données figurant dans des documents d'identité (par exemple, passeport ou carte nationale d'identité) ;
    - ii. soit une photographie de bonne qualité complétée par au moins un élément d'identification tel qu'un « alias », le nom de l'un des deux parents ou un signe physique particulier non présent sur la photographie.

- b) Si la personne n'est pas identifiée :
  - i. une photographie de bonne qualité, et/ou
  - ii. les empreintes digitales, et/ou
  - iii. le profil d'ADN.

#### Article 89 : Notices vertes

1. Les notices vertes sont publiées pour alerter sur les activités criminelles d'une personne.
2. Une notice verte ne peut être publiée qu'aux conditions suivantes :
  - a) la personne est considérée comme constituant une menace pour la sécurité publique ;
  - b) cette conclusion se fonde sur une évaluation effectuée par un service national chargé de l'application de la loi ou par une entité internationale ;
  - c) cette évaluation se fonde sur l'existence d'une ou de plusieurs condamnations antérieures ou sur d'autres motifs raisonnables ;
  - d) suffisamment de données relatives à la menace sont fournies pour que la mise en garde soit pertinente.
3. Une notice verte ne peut être publiée que si elle comporte des éléments d'identification suffisants. Par éléments suffisants, on entend au moins :
  - a) Soit le nom de famille, le prénom, le sexe et la date de naissance (au moins l'année) complétés par la description physique de la personne, le profil d'ADN, les empreintes digitales ou les données figurant dans des documents d'identité (par exemple, passeport ou carte nationale d'identité) ;
  - b) Soit une photographie de bonne qualité complétée par au moins un élément d'identification tel qu'un « alias », le nom de l'un des deux parents ou un signe physique particulier non présent sur la photographie.
4. Les Bureaux centraux nationaux et les entités nationales destinataires des notices vertes prennent les dispositions adéquates, conformément à la législation nationale applicable.

#### Article 90 : Notices jaunes

1. Les notices jaunes sont publiées pour retrouver une personne disparue ou pour identifier une personne dans l'incapacité de s'identifier elle-même.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

2. Une notice jaune ne peut être publiée qu'aux conditions suivantes :
    - a) la disparition ou la découverte de la personne a été signalée et constatée par la police ;
    - b) la police ignore le lieu où se trouve la personne disparue ou l'identité de la personne découverte ;
    - c) si la personne est majeure, la législation nationale applicable relative à la protection de la vie privée n'empêche pas la demande ;
    - d) suffisamment de données relatives à la personne ou aux circonstances de sa disparition ou de sa découverte sont fournies pour permettre une identification.
  3. Une notice jaune ne peut être publiée que si elle comporte des éléments d'identification suffisants. Par éléments suffisants, on entend au moins :
    - a) S'il s'agit d'une personne disparue :
      - i. le nom de famille, le prénom, le sexe et la date de naissance (au moins l'année), et
      - ii. la description physique de la personne, une photographie de bonne qualité, le profil d'ADN ou les empreintes digitales ;
    - b) S'il s'agit d'une personne incapable de s'identifier elle-même :
      - i. la description physique de la personne, le sexe, et
      - ii. une photographie de bonne qualité, les empreintes digitales ou le profil d'ADN.
- Article 91 : Notices noires**
1. Les notices noires sont publiées pour identifier des personnes décédées.
  2. Une notice noire ne peut être publiée qu'aux conditions suivantes :
    - a) la découverte d'un cadavre a été constatée par la police ;
    - b) ce cadavre n'a pu être identifié ;
    - c) suffisamment de données relatives à ce cadavre ou aux circonstances de sa découverte sont fournies pour permettre une identification.

3. Une notice noire ne peut être publiée que si elle comporte des éléments d'identification suffisants. Par éléments suffisants, on entend au moins :
  - a) une photographie de bonne qualité, et/ou
  - b) les empreintes digitales, et/ou
  - c) le profil d'ADN.

## **Article 92 : Notices mauves**

1. Les notices mauves sont publiées pour :
  - a) Alerter sur les modes opératoires, des objets, des dispositifs ou des modes de dissimulation utilisés par des auteurs d'infractions, et/ou
  - b) Solliciter des informations sur des faits criminels aux fins d'élucidation.
2. Une notice mauve ne peut être publiée qu'aux conditions suivantes :
  - a) S'agissant de faits élucidés :
    - i. le mode opératoire utilisé est connu avec précision, complexe ou se distingue d'autres modes opératoires recensés pour des infractions de même nature ;
    - ii. la publication de la notice est de nature à prévenir la réitération de ces infractions ;
    - iii. la demande comporte suffisamment de données relatives au mode opératoire, aux objets, aux équipements ou aux caches utilisés par les auteurs de ces infractions pour permettre une prévention efficace.
    - iv. La demande comporte suffisamment d'éléments permettant d'effectuer des rapprochements avec des faits similaires en vue de leur éventuelle élucidation.
  - b) S'agissant de faits non élucidés :
    - i. les faits criminels sont graves ;
    - ii. les faits permettent d'attirer l'attention des membres de l'Organisation sur un mode opératoire, un objet, un dispositif ou un mode de dissimulation particulier ;
    - iii. la demande comporte suffisamment de données relatives à ce mode opératoire, à ces objets, à ces équipements ou à ces caches pour permettre des rapprochements.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

### **Article 93 : Notices orange**

1. Les notices orange sont publiées pour notifier d'un événement, d'une personne, d'un objet, d'un procédé ou d'un mode opératoire constituant une menace imminente pour la sécurité publique et susceptible de porter gravement atteinte aux personnes ou aux biens.
2. Une notice orange ne peut être publiée qu'aux conditions suivantes :
  - a) dans le cas d'une personne :
    - i. elle est considérée comme constituant une menace imminente pour la sécurité publique ou elle prépare ou s'apprête à commettre de manière imminente une infraction de droit commun d'une particulière gravité ;
    - ii. cette conclusion se fonde sur une évaluation effectuée par un service national chargé de l'application de la loi ou une entité internationale ;
    - iii. cette évaluation se fonde sur l'existence d'une ou de plusieurs condamnations antérieures ou sur d'autres motifs raisonnables.
  - b) dans le cas d'un objet, d'un événement ou d'un mode opératoire :
    - i. il est considéré comme constituant une menace imminente pour la sécurité publique ;
    - ii. cette conclusion se fonde sur une évaluation effectuée par un service national chargé de l'application de la loi.
3. Une notice orange ne peut être publiée que si suffisamment de données relatives à la menace imminente sont fournies pour que la mise en garde soit pertinente.
4. Les Bureaux centraux nationaux et les entités nationales destinataires des notices orange prennent les dispositions adéquates, conformément à la législation nationale applicable.
5. Lorsque la menace ayant justifié la publication d'une notice orange ne revêt plus un caractère imminent, le Secrétariat général, en concertation avec le Bureau central national ou l'entité internationale ayant demandé sa publication, peut procéder à son remplacement par toute autre notice appropriée.

### **Article 94 : Notices œuvres d'art volées [supprimé]**

### **Article 95 : Notices spéciales INTERPOL-Conseil de sécurité des Nations Unies**

1. Les notices spéciales INTERPOL-Conseil de sécurité des Nations Unies sont publiées afin d'informer les Membres de l'Organisation qu'un individu ou une entité fait l'objet de sanctions décidées par le Conseil de sécurité.
2. Les notices spéciales INTERPOL-Conseil de sécurité des Nations Unies sont publiées conformément à l'arrangement relatif à la coopération entre l'Organisation internationale de police criminelle - INTERPOL et l'Organisation des Nations Unies en ce qui concerne les Comités des sanctions du Conseil de sécurité de l'Organisation des Nations Unies.
3. Les conditions de publication de ces notices spéciales sont fixées selon les procédures déterminées d'un commun accord par le Secrétariat de l'Organisation des Nations Unies et INTERPOL, en concertation avec les Comités concernés.

### **Article 96 : Autres notices spéciales**

1. La finalité, les conditions de publication et la structure de toute autre catégorie de notices spéciales sont fixées dans l'accord visé à l'article 28 du présent Règlement, dans le respect des buts et activités de l'Organisation et des principes énoncés au titre 1 du présent Règlement.
2. Une notice spéciale ne peut être publiée que si les données remplissent les conditions nécessaires à la publication de cette catégorie de notices spéciales, telles que précisées dans ledit accord.

## **SECTION 4 : DIFFUSIONS**

### **Article 97 : Système des diffusions**

1. Le système des diffusions est constitué de demandes de coopération et d'alertes correspondant chacune à une finalité spécifique et présentées de manière standardisée :
  - a) arrêter, mettre en détention ou restreindre les déplacements d'une personne condamnée ou accusée ;
  - b) localiser ;

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

- c) obtenir des informations complémentaires ;
  - d) identifier ;
  - e) alerter sur les activités criminelles d'une personne ;
  - f) informer.
2. Les conditions de transmission d'une diffusion correspondent aux conditions générales d'enregistrement des données dans les bases de données de police de l'Organisation.
  3. Le Secrétariat général soumet au Comité exécutif pour approbation tout projet de création d'une nouvelle catégorie de diffusion. Il fournit à l'appui de sa demande :
    - a) les motifs ayant conduit le Secrétariat général à cette création ainsi que les implications financières de celle-ci ;
    - b) la finalité spécifique de cette nouvelle catégorie de diffusion, ses conditions de transmission ainsi que le type des données qu'elle contiendra ;
    - c) le résultat des tests éventuellement conduits par le Secrétariat général ;
    - d) l'avis de la Commission de contrôle des fichiers dès lors que la nouvelle catégorie de diffusion contient des données à caractère personnel ou est reliée à de telles données.

### **Article 98 : Mise à disposition des formulaires de diffusions**

1. Le Secrétariat général est tenu de mettre à la disposition aux Bureaux centraux nationaux et des entités internationales des outils et mécanismes permettant un traitement automatisé et homogène des diffusions dans le Système d'information d'INTERPOL ainsi que leur consultation directe.
2. Le Secrétariat général met à la disposition des Bureaux centraux nationaux et des entités internationales les formulaires leur permettant de transmettre des demandes de coopération et des alertes par voie de diffusion.
3. Le Secrétariat général, en concertation avec les Bureaux centraux nationaux ou avec leurs représentants au sein des organes consultatifs créés à cet effet, définit et modifie, s'il y a lieu, la structure de chaque formulaire.

### **Article 99 : Transmission des diffusions**

1. Les diffusions sont transmises dans au moins une des langues de travail de l'Organisation.

2. Avant de transmettre une diffusion, le Bureau central national ou l'entité internationale s'assure :
  - a) de la qualité et de la licéité des données qu'il ou elle fournit à l'appui de sa diffusion ;
  - b) de la conformité de sa diffusion aux conditions générales d'enregistrement de données ;
  - c) de l'intérêt des données pour la coopération policière internationale ;
  - d) de la conformité de sa diffusion à la réglementation d'INTERPOL, en particulier aux articles 2(1) et 3 du Statut, ainsi qu'aux obligations qui s'imposent à lui ou à elle au regard du droit international.
3. Un Bureau central national ou une entité internationale doit utiliser une diffusion plutôt qu'une notice si il ou elle souhaite :
  - a) limiter la transmission de sa demande de coopération ou de son alerte à des Bureaux centraux nationaux ou à des entités internationales sélectionnés ;
  - b) limiter l'accès aux données contenues dans sa demande de coopération ou dans son alerte à un nombre restreint de Bureaux centraux nationaux ou d'entités internationales ;
  - c) sa demande ou son alerte ne justifie pas la publication d'une notice ou ne remplit pas les conditions requises à cet effet.

### **Article 100 : Suspension ou retrait d'une diffusion**

1. Le Bureau central national ou l'entité internationale ayant transmis une alerte ou une demande de coopération par voie de diffusion peut suspendre sa diffusion pour une période n'excédant pas six mois. Il ou elle indique au Secrétariat général les raisons de cette suspension.
2. Le Bureau central national ou l'entité internationale ayant transmis une alerte ou une demande de coopération par voie de diffusion est tenu d'évaluer le maintien de sa diffusion dès lors que les données contenues dans ladite diffusion sont modifiées.
3. Le Bureau central national ou l'entité internationale ayant transmis une alerte ou une demande de coopération par voie de diffusion est tenu de notifier le retrait de sa diffusion aux Bureaux centraux nationaux et aux entités internationales ainsi qu'au Secrétariat général dès lors que celle-ci a atteint sa finalité ou qu'il ou elle ne souhaite plus la maintenir.

**Article 101 : Enregistrement de demandes de coopération ou alertes transmises par voie de message**

1. Conformément à l'article 9(4) du présent Règlement, un Bureau central national ou une entité internationale peut demander au Secrétariat général d'enregistrer dans une base de données de police de l'Organisation une demande de coopération ou une alerte internationale qu'il ou elle a transmis initialement par voie de message et dont le Secrétariat général n'était pas initialement destinataire.
2. Le Secrétariat général procède à l'enregistrement de ladite demande de coopération ou de ladite alerte conformément aux dispositions du présent Règlement et conformément aux restrictions d'accès et aux conditions d'utilisation des données éventuellement fixées par le Bureau central national ou l'entité internationale.

**SECTION 5 :  
NOTICES ET DIFFUSIONS À L'INITIATIVE  
DU SECRÉTARIAT GÉNÉRAL**

**Article 102 : Sollicitations d'informations**

1. Le Secrétariat général peut solliciter auprès des sources des informations aux fins de coopération dans les cas suivants :
  - a) sa démarche s'inscrit dans le cadre d'un projet déterminé ou d'un événement présentant un intérêt pour la coopération policière internationale ;
  - b) il a des raisons d'estimer que cela est nécessaire pour la poursuite des objectifs de l'Organisation et est proportionné aux buts poursuivis.
2. Le Secrétariat général doit avoir obtenu l'autorisation préalable du Bureau central national de toute entité nationale auprès de qui il souhaite solliciter des informations. L'autorisation du Bureau central national est présumée lorsque ledit Bureau n'a pas répondu au Secrétariat général dans un délai de 30 jours à compter de la demande d'autorisation. Il est entendu que ce bureau conserve la possibilité de s'opposer à tout moment à une telle demande d'information auprès d'une de ses entités nationales.

**Article 103 : Publication de notices**

1. Conformément à l'article 25(4) du présent Règlement, le Secrétariat général peut publier des notices de sa propre initiative :
  - a) à des fins d'alerte ;
  - b) pour solliciter des informations.

2. Avant de publier une notice de sa propre initiative, le Secrétariat général s'assure que :
  - a) la publication de la notice est conforme aux conditions de publication de ladite notice ;
  - b) la ou les sources des données ont consenti à cette publication, en particulier que toute restriction d'accès a été levée et que le niveau de confidentialité fixé pour ces données permet cette publication ;
  - c) la publication de la notice n'est pas de nature à interférer avec une demande de coopération en cours ou qu'aucune demande de notice similaire n'a été soumise par un Bureau central national ou une entité internationale.

**SECTION 6 :  
SIGNALEMENTS POSITIFS**

**Article 104 : Génération de signalements positifs**

1. Un signalement positif est généré dans le Système d'information d'INTERPOL à chaque fois qu'une concordance suffisante est établie entre la consultation et des données enregistrées dans une base de données de police opérationnelles permanente de l'Organisation. L'établissement d'une concordance suffisante dépend des caractéristiques de chaque base de données.
2. Lorsqu'un signalement positif est généré, sous réserve des caractéristiques de chaque base de données, une notification est envoyée au Bureau central national ou à l'entité internationale qui a effectué la consultation, ainsi qu'au Secrétariat général. Une notification est également envoyée au Bureau central national ou à l'entité internationale qui a enregistré les données initiales, selon les préférences qu'ils ont indiquées concernant la réception des notifications de signalements positifs.
3. La notification du signalement positif comprend au minimum la référence du Bureau central national ou de l'entité internationale qui a effectué la consultation et celle du Bureau central national ou de l'entité internationale qui a enregistré les données initiales, ainsi que les données principales relatives à la personne, à l'objet ou à l'événement faisant l'objet de l'enregistrement.
4. Lorsque les données sont traitées par des entités privées dans le cadre de projets spécifiques, l'ensemble des conditions et modalités relatives aux signalements positifs sont définies dans les accords conclus entre l'Organisation et lesdites entités, en application de l'article 28 du présent Règlement.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

### Article 105 : Procédure de traitement de signalements positifs

1. Le Bureau central national ou l'entité internationale qui a généré le signalement positif prend contact avec le Bureau central national ou avec l'entité internationale qui a enregistré les données initiales conformément à l'article 63(1).
2. Le Bureau central national ou l'entité internationale qui a enregistré les données initiales examine la pertinence du signalement positif dans les meilleurs délais.
3. Des procédures sont définies par le Secrétariat général, en concertation avec les Bureaux centraux nationaux ou avec leurs représentants au sein des organes consultatifs créés à cet effet, pour définir les mesures à prendre et délais de réponse selon la nature de la demande de coopération.
4. Les Bureaux centraux nationaux déterminent les modalités selon lesquelles les signalements positifs sont notifiés à leurs entités nationales, dans le respect du droit national applicable.

### Article 106 : Relevés des signalements positifs

1. Le Secrétariat général conserve un relevé des signalements positifs générés pour une demande de coopération donnée. Ce relevé est conservé pendant la durée de l'enregistrement des données dans les bases de données de police.
2. Ce relevé est consultable par le Bureau central national ou l'entité internationale qui a enregistré les données initiales.

## CHAPITRE III : SÉCURITÉ DES DONNÉES

### SECTION 1 : GESTION DES DROITS D'ACCÈS AU SYSTÈME D'INFORMATION D'INTERPOL

### Article 107 : Désignation d'un nouveau Bureau central national

1. Le Secrétariat général informe les Bureaux centraux nationaux et les entités internationales de toute nouvelle adhésion à l'Organisation et de la désignation d'un Bureau central national.

2. À compter de la notification du Secrétariat général, un Bureau central national ou une entité internationale dispose de 45 jours pour s'opposer à toute possibilité de traitement par ce Bureau central national des données qu'il ou elle a enregistrées dans les bases de données de police.

### Article 108 : Octroi d'un accès à une nouvelle entité nationale

1. Préalablement à l'octroi de l'accès au Système d'information d'INTERPOL à une nouvelle entité nationale, le Bureau central national prend les mesures nécessaires pour s'assurer que ladite entité nationale respectera les obligations nées du présent Règlement.
2. Chaque Bureau central national notifie au Secrétariat général tout accès au Système d'information d'INTERPOL qu'il a conféré à une nouvelle entité nationale.
3. Il précise l'étendue des autorisations conférées.

### Article 109 : Octroi d'un accès à une nouvelle entité internationale

1. Le Secrétariat général notifie aux Bureaux centraux nationaux et aux entités internationales tout accès octroyé par l'Organisation à une nouvelle entité internationale.
2. Il précise l'étendue des autorisations conférées au titre de l'accord conclu avec l'Organisation.
3. À compter de la notification du Secrétariat général, un Bureau central national ou une entité internationale dispose de 45 jours pour s'opposer à toute possibilité d'accès par cette entité internationale aux données qu'il ou elle a enregistrées dans les bases de données de police.

### Article 110 : Registre des accès au Système d'information d'INTERPOL

Le Secrétariat général tient à jour le registre de tous les Bureaux centraux nationaux, de toutes les entités nationales, de toutes les entités internationales et de toutes les entités privées autorisés à traiter, directement ou indirectement, des données dans le Système d'information d'INTERPOL et le met à disposition de manière permanente. Ce registre précise la finalité, la nature et l'étendue des possibilités de traitement accordées et tout changement récent dans ces possibilités.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

### Article 111 : Droits d'accès individuels au Système d'information d'INTERPOL

1. Conformément à l'article 15(4) et (5) du présent Règlement, les droits d'accès au Système d'information d'INTERPOL sont octroyés à des personnes expressément autorisées, uniquement en fonction du besoin d'en connaître et en tenant compte des niveaux de confidentialité.
2. Ils sont déterminés :
  - a) par les Bureaux centraux nationaux pour leur personnel et celui de leurs entités nationales ;
  - b) par le Secrétariat général pour son personnel et le personnel des entités internationales.
3. Les Bureaux centraux nationaux et les entités internationales sont tenus de prendre toute mesure appropriée pour que les utilisateurs du Système d'information d'INTERPOL qu'ils autorisent respectent les dispositions du présent Règlement.
4. Les Bureaux centraux nationaux et les entités internationales doivent :
  - a) mettre en œuvre tout moyen approprié pour que les utilisateurs autorisés connaissent et puissent respecter les dispositions du présent Règlement, et qu'à cette fin, ils reçoivent la formation nécessaire ;
  - b) retransmettre aux utilisateurs autorisés les informations transmises par le Secrétariat général.
5. Les Bureaux centraux nationaux, les entités internationales et le Secrétariat général tiennent un registre des noms des personnes et des droits d'accès octroyés. Ils indiquent à quelle(s) base(s) de données et à quelle(s) donnée(s) ils autorisent l'utilisateur à accéder.
6. Un Bureau central national peut choisir de déléguer à une entité nationale la gestion des droits d'accès des utilisateurs de cette entité nationale. Il veille à ce que ladite entité nationale respecte les obligations ci-dessus. Les modalités de cette délégation sont définies dans l'accord conclu entre le Bureau central national et l'entité nationale conformément à l'article 21(3) du présent Règlement. Le Bureau central national procède à des vérifications régulières du respect par l'entité de ces obligations et des modalités définies.

### **SECTION 2 : RESPECT DE LA CONFIDENTIALITÉ**

#### Article 112 : Niveaux de confidentialité

1. Il existe trois niveaux de confidentialité, correspondant aux risques croissants liés à la divulgation non autorisée des données :
  - a) « À USAGE OFFICIEL INTERPOL UNIQUEMENT »
  - b) « DIFFUSION RESTREINTE INTERPOL »
  - c) « CONFIDENTIEL INTERPOL ».
2. Les données sont classées :
  - a) « À USAGE OFFICIEL INTERPOL UNIQUEMENT » si leur divulgation non autorisée est de nature à entraver l'action des services chargés de l'application de la loi ou bien à désavantager ou à discréditer l'Organisation, son personnel, ses Membres, les Bureaux centraux nationaux, les entités nationales, les entités internationales ou les personnes que lesdites données concernent ;
  - b) « DIFFUSION RESTREINTE INTERPOL » si leur divulgation non autorisée est susceptible de compromettre l'action des services chargés de l'application de la loi ou bien de nuire à l'Organisation ou à son personnel, à ses Membres, aux Bureaux centraux nationaux, aux entités nationales, aux entités internationales ou aux personnes que lesdites données concernent ;
  - c) « CONFIDENTIEL INTERPOL » si leur divulgation non autorisée est susceptible de compromettre gravement l'action des services chargés de l'application de la loi ou bien de nuire gravement à l'Organisation ou à son personnel, à ses Membres, aux Bureaux centraux nationaux, aux entités nationales, aux entités internationales ou aux personnes que lesdites données concernent.
3. Si la source des données ne leur a attribué aucun niveau de confidentialité, ces données sont classées « À USAGE OFFICIEL INTERPOL UNIQUEMENT ».
4. Si un Bureau central national, une entité nationale ou une entité internationale a besoin, dans un cas particulier, d'attribuer à certaines données un niveau de confidentialité plus élevé que ceux indiqués ci-dessus, le Secrétariat général en étudie la possibilité avec ledit Bureau central national ou ladite entité. Dans l'affirmative, ils concluent un accord spécial définissant les conditions attachées au traitement de ces données.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

5. Un Bureau central national, une entité nationale ou une entité internationale peut à tout moment modifier le niveau de confidentialité qu'il ou elle a attribué à des données, notamment en leur attribuant un niveau de confidentialité inférieur à celui précédemment indiqué si il ou elle considère que la protection à apporter aux données peut être moindre.
3. Le Secrétariat général élabore les procédures de traitement administratives et techniques qui doivent être observées par son personnel pour chaque niveau de confidentialité.

### **Article 113 : Mesures supplémentaires prises par le Secrétariat général**

1. Le Secrétariat général peut, avec le consentement du Bureau central national, de l'entité nationale ou de l'entité internationale qui a procédé à l'enregistrement de données, attribuer à ces données un niveau de confidentialité supérieur à celui indiqué par la source, au regard des risques que son traitement, et plus particulièrement sa divulgation, peuvent faire courir à la coopération policière internationale ou à l'Organisation, son personnel et ses Membres.
4. Les Bureaux centraux nationaux, les entités nationales et les entités internationales mettent en place en leur sein des procédures de traitement administratives et techniques au moins équivalentes à celles du Secrétariat général afin de s'assurer du respect du niveau de confidentialité demandé par le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à l'enregistrement des données.
5. Le Secrétariat général définit, en coordination avec les Bureaux centraux nationaux et les entités concernées, des tables d'équivalence entre les niveaux de classification qu'il applique et ceux appliqués par les Bureaux centraux nationaux, les entités nationales et les entités internationales, chaque fois que cela s'avère nécessaire.

2. Le Secrétariat général détermine, de la même manière, le niveau de confidentialité de la plus-value qu'il apporte aux données, notamment lorsqu'il réalise un travail d'analyse ou publie une notice. Dans ce cas, il avise la ou les sources des données de cette mesure supplémentaire.
3. Le Secrétariat général peut également classifier une base de données dans les mêmes conditions que celles indiquées ci-dessus.
4. Le Secrétariat général, lorsqu'il a attribué à des données un niveau de confidentialité supérieur à celui indiqué par le Bureau central national, l'entité nationale ou l'entité internationale qui a procédé à leur enregistrement, peut à tout moment modifier ce niveau de confidentialité supérieur.

### **Article 114 : Respect de la confidentialité dans le Système d'information d'INTERPOL**

1. Le Secrétariat général est responsable de la définition de procédures d'autorisation ou d'habilitation de sécurité pour chaque niveau de confidentialité des données. L'accès à un niveau de confidentialité donné s'entend sous réserve des restrictions définies par les Bureaux centraux nationaux, les entités internationales ou le Secrétariat général.
2. Les équipements et l'infrastructure de communication utilisés aux fins du traitement des données sont dotés, selon le niveau de confidentialité attribué aux données, de dispositifs de sécurité permettant de prévenir le risque de divulgation non autorisée ou de détecter une telle divulgation.

3. Le Secrétariat général élabore les procédures de traitement administratives et techniques qui doivent être observées par son personnel pour chaque niveau de confidentialité.
4. Le Secrétariat général définit, en coordination avec les Bureaux centraux nationaux et les entités concernées, des tables d'équivalence entre les niveaux de classification qu'il applique et ceux appliqués par les Bureaux centraux nationaux, les entités nationales et les entités internationales, chaque fois que cela s'avère nécessaire.

## **SECTION 3 : GESTION DU SYSTÈME DE SÉCURITÉ**

### **Article 115 : Règles de sécurité**

1. Conformément à l'article 15 du présent Règlement, le Secrétariat général définit des règles de sécurité établissant des dispositifs de sécurité techniques et administratifs à même de garantir des niveaux appropriés de confidentialité, d'intégrité et de disponibilité pour le Système d'information d'INTERPOL.
2. Le Secrétariat général procède à l'évaluation des risques nécessaire.
3. Le Secrétariat général met en place les dispositifs de contrôle qui conviennent pour que la sécurité des données soit assurée.
4. Le Secrétariat peut si nécessaire définir des règles de sécurité particulières pour une partie de l'infrastructure de communication, une base de données ou un service spécifique.

### **Article 116 : Mise en œuvre par les Bureaux centraux nationaux et les entités**

Il appartient aux Bureaux centraux nationaux, aux entités nationales et aux entités internationales d'adopter un niveau de sécurité approprié qui soit au moins équivalent au niveau minimum fixé par les règles en la matière instaurées par le Secrétariat général.

**Article 117 : Désignation d'un officier de sécurité**

1. Chaque Bureau central national, chaque entité nationale ou chaque entité internationale désigne un ou plusieurs officiers de sécurité chargés des opérations de sécurité pour leur pays ou organisation internationale dans le Système d'information d'INTERPOL.
2. L'officier de sécurité s'assure en particulier :
  - a) du respect des procédures de sécurité établies par son Bureau central national, son entité nationale ou son entité internationale ;
  - b) de la mise à jour desdites procédures, notamment au regard des règles instaurées par le Secrétariat général ;
  - c) de la formation continue, en matière de sécurité des données, du personnel de son Bureau central national, de son entité nationale ou de son entité internationale.
3. En tant que de besoin, l'officier de sécurité collabore avec l'officier délégué à la protection des données.
4. L'officier de sécurité assure la coordination avec le Secrétariat général, suivant nécessité, pour ce qui est des questions de sécurité.

**SECTION 4 :  
INCIDENTS DE SÉCURITÉ**

**Article 118 : Information relative à un incident de sécurité**

1. En cas d'intrusion ou de tentative d'intrusion grave dans le réseau ou dans une base de données de l'Organisation, ou encore d'atteinte ou de tentative d'atteinte à l'intégrité ou à la confidentialité des données, le Secrétariat général est tenu d'en informer la source desdites données, le Bureau central national si elle touche une entité nationale qu'il a autorisée, le Comité exécutif et la Commission de contrôle des fichiers.
2. En cas d'atteinte ou de tentative d'atteinte à l'intégrité ou à la confidentialité des données initialement traitées dans le Système d'information d'INTERPOL et traitées dans le système d'information d'un Bureau central national ou d'une entité internationale, il ou elle est tenu d'en informer la source desdites données et le Secrétariat général ainsi que la Commission de contrôle des fichiers lorsque l'incident de sécurité concerne des données à caractère personnel. Lorsque l'atteinte ou la tentative d'atteinte survient dans le système d'information d'une entité nationale, le Bureau central national qui l'a autorisée à accéder au Système d'information d'INTERPOL veille à en informer la source et le Secrétariat général.

**Article 119 : Restauration partielle ou totale du Système d'information d'INTERPOL**

Le Secrétariat général entreprend toute démarche nécessaire et appropriée en vue d'être à même de restaurer dans les plus brefs délais, en cas de dommage, le fonctionnement régulier du Système d'information d'INTERPOL, en particulier ses bases de données et son infrastructure de communication.

**TITRE 4 :  
CONTRÔLES**

**CHAPITRE I :  
NATURE DES CONTRÔLES**

**Article 120 : Contrôle des utilisateurs**

1. Les Bureaux centraux nationaux, les entités nationales et les entités internationales sont tenus de s'assurer régulièrement que leurs utilisateurs respectent le présent Règlement et, en particulier, en ce qui concerne la qualité des données qu'ils introduisent dans le système et l'utilisation qu'ils font des données consultées dans celui-ci. Les contrôles sont effectués dans le cadre de vérifications d'office ou d'incidents de traitement.
2. Ils prennent, dans la limite du présent Règlement, toute mesure afin de corriger ou de faire corriger une possible erreur de traitement.

**Article 121 : Désignation d'un officier délégué à la protection des données au sein des Bureaux centraux nationaux et des entités nationales et internationales**

1. Tout Bureau central national, toute entité nationale et toute entité internationale désigne un officier délégué à la protection des données chargé de l'organisation et de la mise en œuvre des contrôles ci-dessus. La fonction d'officier délégué à la protection des données sera normalement exercée distinctement de celle d'officier de sécurité.
2. L'officier délégué à la protection des données s'assure en particulier :
  - a) de l'établissement au sein de son Bureau central national, de son entité nationale ou de son entité internationale de procédures de traitement conformes au présent Règlement ;
  - b) de la mise en œuvre de contrôles dans le cadre de vérifications d'office ou d'incidents de traitement destinés à garantir le respect du Règlement et desdites procédures ;

- c) de la mise à jour desdites procédures et mécanismes ;
  - d) de la mise en œuvre de programmes de formation continue adéquats, en matière de traitement des données, à l'intention du personnel de son Bureau central national, de son entité nationale ou de son entité internationale.
3. En tant que de besoin, l'officier délégué à la protection des données collabore avec l'officier de sécurité et avec l'officier délégué à la protection des données d'INTERPOL.
- Article 121A : Désignation d'un officier délégué à la protection des données au sein du Secrétariat général**
- 1. Conformément à l'article 29 du Statut d'INTERPOL et aux articles 17(5,6) et 22(1,5) du présent Règlement, le Secrétaire Général, après consultation du Comité exécutif et de la Commission de contrôle des fichiers d'INTERPOL, nomme un officier délégué à la protection des données ci-après dénommé « le Délégué à la protection des données d'INTERPOL (IDPO) ».
  - 2. Le Délégué à la protection des données d'INTERPOL (IDPO) est nommé pour une durée de cinq ans reconductible une fois.
  - 3. Le Délégué à la protection des données d'INTERPOL (IDPO) exerce ses fonctions en toute indépendance et est placé sous l'autorité directe du Secrétaire Général.
  - 4. Le Délégué à la protection des données d'INTERPOL (IDPO) remplit en particulier les fonctions suivantes :
    - a) Il contrôle la licéité et la conformité du traitement des données dans le Système d'information d'INTERPOL comme le prévoient le Statut et les règlements de l'Organisation ;
    - b) Il conseille les Bureaux centraux nationaux ou les autres entités qui utilisent le Système d'information d'INTERPOL, de sa propre initiative ou à la demande du Secrétariat général, au sujet des opérations de traitement susceptibles de présenter un risque important pour les droits et libertés des individus, notamment en matière d'analyses d'impact relatives à la protection des données, et il contrôle les mesures prises à la suite de ses conseils ;
    - c) Il assure la liaison avec tous les officiers délégués à la protection des données désignés en application de l'article 121 du présent Règlement, collabore et assure la coordination avec eux, notamment par des formations et par la sensibilisation aux questions de protection des données ;
    - d) Il étudie les rapports présentés chaque année par les officiers délégués à la protection des données conformément aux articles 17(4, 5, 6) et 123(3) du présent Règlement ;
    - e) Il forme et sensibilise le personnel du Secrétariat général sur les questions de traitement des données ;
    - f) Il assure la liaison avec la Commission de contrôle des fichiers d'INTERPOL sur les questions de traitement des données ;
    - g) Il assure la liaison avec les officiers délégués à la protection des données d'autres institutions et organisations, en particulier par l'échange d'expertise et de bonnes pratiques.
  - 5. Pour s'acquitter efficacement de ses fonctions, le Délégué à la protection des données d'INTERPOL (IDPO) dispose d'un droit d'accès libre et sans restrictions à toutes les données traitées dans le Système d'information d'INTERPOL et à tout système de traitement de ces données au sein de ce dernier, quels que soient le lieu, la forme ou le support dudit traitement.
  - 6. Dans l'exercice de ses fonctions, le Délégué à la protection des données d'INTERPOL (IDPO) peut présenter au Secrétariat général :
    - a) des recommandations sur les mesures à prendre concernant les questions de traitement des données au sein du Secrétariat général, notamment la correction des erreurs de traitement ;
    - b) des recommandations quant à la nécessité de prendre des mesures correctives comme le prévoit l'article 131 du présent Règlement ;
    - c) des rapports sur la non-application des recommandations du Délégué à la protection des données d'INTERPOL (IDPO) au sein du Secrétariat général.
  - 7. Le Délégué à la protection des données d'INTERPOL (IDPO) peut, de sa propre initiative ou à la demande de Commission de contrôle des fichiers d'INTERPOL, communiquer à celle-ci les recommandations formulées et les rapports publiés, pour information ou en vue de toute autre action que la Commission juge appropriée.
  - 8. Le Délégué à la protection des données d'INTERPOL (IDPO) peut solliciter l'avis d'experts extérieurs sur les questions générales en rapport avec ses fonctions.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

9. Le Délégué à la protection des données d'INTERPOL (IDPO) présente chaque année un rapport au Comité exécutif. Ce rapport est mis à la disposition de la Commission de contrôle des fichiers d'INTERPOL.
10. Le Secrétaire Général adopte des règles d'application portant sur le travail du Délégué à la protection des données d'INTERPOL (IDPO), notamment sur les fonctions particulières relevant de sa mission, les procédures internes et les garanties d'indépendance du Délégué à la protection des données d'INTERPOL (IDPO).

### **Article 122 : Contrôle de l'utilisation des données**

1. Tout Bureau central national peut demander des informations sur l'utilisation faite par un autre Bureau central national, une entité nationale ou une entité internationale des données qu'une de ses entités nationales ou que lui-même a traité dans le Système d'information d'INTERPOL. Si les données ont été consultées ou utilisées par une entité nationale, il procède au contrôle par l'intermédiaire du Bureau central national de cette entité nationale. Si les données ont été consultées ou utilisées par une entité internationale, il procède au contrôle par l'intermédiaire du Secrétariat général.
2. Le Secrétariat général assiste les entités internationales dans l'exercice de ce même droit de contrôle.
3. Le Bureau central national, l'entité nationale ou l'entité internationale qui fait l'objet du contrôle est tenu de fournir les données demandées.

### **Article 123 : Évaluation des entités nationales**

1. Conformément à l'article 17(4) du présent Règlement, les Bureaux centraux nationaux procèdent à l'évaluation au regard du présent Règlement du fonctionnement des entités nationales qu'ils ont autorisées à accéder directement au Système d'information d'INTERPOL.
2. Le respect par une entité nationale de ses obligations au regard du présent Règlement est une condition essentielle pour que ladite entité nationale puisse conserver l'accès direct au Système d'information d'INTERPOL.
3. Tout Bureau central national fait rapport chaque année au Secrétariat général sur les vérifications d'office auxquelles il a procédé, les incidents de traitement qu'il a traités, les actions de formation de personnel qu'il a réalisées et les mesures nouvelles qu'il a adoptées pour satisfaire aux obligations du Règlement.

4. Le Secrétariat général est habilité à demander au Bureau central national de prendre des mesures correctives à l'encontre de l'entité nationale ou à mettre fin à l'accès au Système d'information d'INTERPOL en cas de traitement de données non conforme et répété par ladite entité, d'absence d'évaluation par ledit Bureau central national ou d'évaluation insuffisante par ce même Bureau central national.

### **Article 124 : Évaluation des Bureaux centraux nationaux**

1. Conformément à l'article 17(5) du présent Règlement, le Secrétariat général procède à l'évaluation au regard du présent Règlement du fonctionnement des Bureaux centraux nationaux.
2. L'évaluation des Bureaux centraux nationaux au regard du présent Règlement est effectuée par le Secrétariat général d'après les directives arrêtées par l'Assemblée générale.

## **CHAPITRE II : OUTILS DE CONTRÔLE**

### **Article 125 : Base de gestion de la conformité**

1. Conformément à l'article 10(4) du présent Règlement, le Secrétariat général peut créer toute base de données afin de s'assurer que les données enregistrées dans les bases de données de police de l'Organisation sont conformes au présent Règlement ou d'éviter un traitement non autorisé ou erroné des données dans lesdites bases de données.
2. La création d'une base de gestion de la conformité s'effectue aux conditions suivantes :
  - a) Elle ne doit contenir que les données nécessaires pour éviter tout traitement non autorisé ou erroné ;
  - b) La conservation des données dans cette base de données est limitée à une durée maximale déterminée par le Comité exécutif. Cette durée peut être prolongée, après notification de la Commission de contrôle des fichiers, si au terme de cette période, l'examen de la gestion de la conformité n'est pas achevé ;
  - c) L'accès à ces bases de données est limité à des services ou à des membres du personnel autorisés du Secrétariat général participant au traitement des données et titulaires d'une autorisation d'accès spécifique.

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

3. Lorsque le Secrétariat général efface des données d'une base de données de police ou d'une base de données de gestion de la conformité, il peut néanmoins conserver, pour une durée maximale déterminée par le Comité exécutif, celles de ces données permettant d'éviter tout traitement non autorisé ou erroné desdites données.

### Article 126 : Registre des opérations de traitement

1. Conformément à l'article 13 du présent Règlement, le Secrétariat général tient un registre des opérations de traitement effectuées dans le Système d'information d'INTERPOL. En particulier, il conserve le relevé des :
  - a) accès au Système d'information d'INTERPOL par les utilisateurs ;
  - b) enregistrements effectués par les utilisateurs ;
  - c) mises à jour effectuées par les utilisateurs ;
  - d) décisions de conservation prises par les utilisateurs ;
  - e) décisions d'effacement prises par les utilisateurs ;
  - f) consultations en accès direct effectuées par les utilisateurs ;
  - g) demandes d'informations reçues et des réponses effectuées.
2. Le relevé contient les seules données nécessaires à l'exercice du contrôle de la conformité du traitement au présent Règlement. Il contient à cet effet : l'identifiant de l'utilisateur, le nom de son Bureau central national, de son entité nationale ou de son entité internationale, la nature de l'opération de traitement effectuée, sa date, la base de données concernée ainsi que les éléments supplémentaires destinés au contrôle.
3. Ces relevés sont conservés pendant une période n'excédant pas la durée maximale déterminée par le Comité exécutif.
4. Ces relevés sont accessibles :
  - a) aux seules fins de contrôle ;
  - b) par le personnel du Secrétariat général habilité aux opérations de contrôle ;
  - c) par la source, à des fins de contrôle, sur demande adressée au Secrétariat général.
5. Ces relevés ne peuvent pas être utilisés aux fins d'une enquête criminelle sauf si cette enquête est liée à l'exercice du contrôle de la conformité du traitement de données au présent Règlement.

### Article 127 : Comparaison de données à des fins de vérification

1. Tout Bureau central national, toute entité nationale ou toute entité internationale ayant traité dans son système d'information des données initialement traitées dans le Système d'information d'INTERPOL peut transmettre au Secrétariat général une demande de comparaison de ces données avec celles actuellement contenues dans le Système d'information d'INTERPOL afin d'en vérifier la qualité. Toute demande émanant d'une entité nationale doit être transmise par l'intermédiaire de son Bureau central national.
2. Toute opération de comparaison de données à des fins de vérification peut être effectuée par voie de téléversement ou de téléchargement :
  - a) Toute opération de comparaison de données par voie de téléversement doit répondre aux conditions cumulatives suivantes :
    - i. le téléversement est effectué uniquement afin de permettre au Secrétariat général de vérifier, pour le compte du Bureau central national, de l'entité nationale ou l'entité internationale qui a transmis la demande, la qualité des données qu'il ou elle a introduites dans son système d'information ;
    - ii. les données téléversées ne sont pas recopiées au sein du Système d'information d'INTERPOL dans lequel elles sont téléversées ;
    - iii. les données téléversées sont systématiquement effacées au terme de l'opération de comparaison.
  - b) Toute opération de comparaison de données par voie de téléchargement doit répondre aux conditions cumulatives suivantes :
    - i. le téléchargement est effectué uniquement afin de permettre à un Bureau central national, à une entité nationale ou à une entité internationale de vérifier la qualité des données qu'il ou elle a introduites dans son système d'information ;
    - ii. le système d'information du Bureau central national, de l'entité nationale ou de l'entité internationale offre un niveau de sécurité au moins équivalent à celui du Système d'information d'INTERPOL ;
    - iii. les données téléchargées ne sont pas recopiées au sein du système d'information dans lequel elles sont téléchargées ;

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

- iv. les données téléchargées sont systématiquement effacées au terme de l'opération de comparaison.
3. Le Secrétariat général est habilité à autoriser une opération de comparaison à des fins de vérification sous réserve :
- du respect des conditions ci-dessus, et
  - d'assurances écrites données par le Bureau central national ou l'entité internationale qui a demandé à procéder à une opération de comparaison de données selon lesquelles il ou elle respectera lesdites conditions, la finalité de l'opération, sa nature et son étendue, et
  - de la désignation d'un responsable de l'opération de comparaison de données au sein du Bureau central national, de l'entité nationale ou de l'entité internationale.
4. Le Secrétariat général tient à jour le registre des opérations de comparaison par voie de téléchargement ou de téléversement.

### CHAPITRE III : MESURES DE CONTRÔLE

#### Article 128 : Procédure d'examen

- Les données sont a priori considérées comme exactes et pertinentes, lorsqu'elles sont introduites dans le Système d'information d'INTERPOL par un Bureau central national, une entité nationale ou une entité internationale et qu'elles ont été enregistrées dans une base de données de police de l'Organisation.
- En cas de doute quant au respect des conditions de traitement des données, le Secrétariat général consulte le Bureau central national concerné, y compris si les données ont été enregistrées par une entité nationale, afin d'obtenir des clarifications ou des données complémentaires susceptibles de lever le doute. Le Secrétariat général consulte également toute entité internationale en cas de doute quant au respect des conditions de traitement des données.
- Le Secrétariat général entreprend toute autre démarche appropriée en vue de s'assurer que ces conditions sont effectivement remplies.
- La procédure d'examen est réputée close lorsque le Secrétariat général conclut que le traitement des données :
  - est conforme au présent Règlement et valide l'enregistrement des données ;
  - n'est pas conforme au présent Règlement et décide d'apporter des corrections au traitement des données ou de procéder à leur effacement.

5. Le Secrétariat général informe le Bureau central national ou l'entité internationale de la fin de la procédure d'examen. S'il a décidé d'apporter des corrections aux données ou de procéder à leur effacement, il en indique les raisons et les corrections apportées audit Bureau central national ou à ladite entité internationale.

#### Article 129 : Mesures conservatoires

- En cas de doute quant au respect des conditions de traitement des données, le Secrétariat général prend toute mesure conservatoire appropriée afin de prévenir tout préjudice direct ou indirect pour l'Organisation, son personnel, ses Membres, les Bureaux centraux nationaux, les entités nationales et internationales ou les personnes que lesdites données concernent.
- Le Secrétariat général informe le Bureau central national ou l'entité internationale de toute mesure conservatoire prise et en indique les raisons.

#### Article 130 : Mesures applicables aux utilisateurs

En cas de violation par un utilisateur des règles applicables au traitement des données dans le Système d'information d'INTERPOL, le Secrétariat général peut :

- demander au Bureau central national ou à l'entité internationale de suspendre ou retirer les droits d'accès qu'il ou elle lui a octroyés ;
- procéder lui-même à cette suspension ou à ce retrait. Il en informe ledit bureau ou ladite entité internationale.

#### Article 131 : Mesures correctives applicables aux Bureaux centraux nationaux et aux entités internationales

- Si un Bureau central national ou une entité internationale rencontre des difficultés au regard du traitement des données dans le Système d'information d'INTERPOL ou ne s'acquitte pas de ses obligations au titre du présent Règlement, le Secrétariat général est habilité à prendre les mesures correctives suivantes :
  - correction des erreurs de traitement ;
  - supervision, pendant une période n'excédant pas trois mois, des opérations de traitement effectuées par le Bureau central national ou l'entité internationale ;
  - suspension de droits d'accès octroyés à des utilisateurs du Bureau central national ou de l'entité internationale ;

## RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES

---

- d) envoi d'une mission d'évaluation du Bureau central national ou de l'entité internationale.
2. Le Secrétariat général peut adresser aux Bureaux centraux nationaux et aux entités internationales des recommandations relatives à la mise en œuvre du présent Règlement en vue de leur permettre, notamment dans le cadre de la formation du personnel ou du renforcement des procédures de travail, de résoudre les difficultés ou de mettre fin aux incidents de traitement.
3. Le Secrétariat général soumet au Comité exécutif pour décision toute proposition de mesures correctives qui auraient pour effet de suspendre de manière prolongée les droits de traitement suivants d'un Bureau central national ou d'une entité internationale :
- droit d'enregistrer des données dans une ou plusieurs bases de données de police de l'Organisation ;
  - droit de consulter une ou plusieurs bases de données ;
  - autorisations d'interconnexion ou de téléchargement.
4. À chaque fois que cela s'avère nécessaire et au moins une fois par an, le Secrétariat général rappelle aux Bureaux centraux nationaux et aux entités internationales leur rôle et leurs responsabilités liées aux données qu'ils ou elles traitent dans le Système d'information d'INTERPOL.

## TITRE 5 : DISPOSITIONS FINALES

### CHAPITRE I : TRAITEMENT DANS TOUT AUTRE BUT LÉGITIME

#### Article 132 : Définition du traitement dans tout autre but légitime

- Conformément à l'article 10(7) du présent Règlement, lorsque des données sont effacées d'une base de données de police de l'Organisation ou d'une base de gestion de la conformité, le Secrétariat général peut néanmoins conserver les données nécessaires à la poursuite de tout autre but légitime.
- Par tout autre but légitime, on entend :
  - la défense des intérêts de l'Organisation, de ceux de ses Membres ou de son personnel, notamment dans le cadre de procédures contentieuses ou précontentieuses et de transactions ;
  - la recherche et la publication scientifiques, historiques, ou journalistiques ;
  - la tenue de statistiques.

- Lorsque des données initialement traitées à des fins de coopération policière sont ultérieurement traitées dans tout autre but légitime, elles ne peuvent plus en aucune manière être utilisées à des fins de coopération policière et ne doivent pas figurer dans les bases de données de police de l'Organisation.
- Le traitement de données à caractère personnel effectué en application du paragraphe 2(b) est seul soumis à l'autorisation préalable de la source des données. Toutefois, lorsque des données à caractère personnel ont été traitées en application du paragraphe 2(a) ci-dessus, la source des données est avisée de leur utilisation ou transmission par le Secrétariat général.
- Le Secrétariat général prend les mesures techniques et organisationnelles nécessaires, notamment en matière de sécurité, propres à garantir que ce traitement ultérieur n'est pas incompatible avec le traitement initial.

#### Article 133 : Les conditions de traitement

- Le traitement des données dans tout autre but légitime doit être motivé. La finalité spécifique de ce traitement doit être clairement indiquée et le traitement limité aux seules données strictement nécessaires à ladite finalité.
- Le traitement est effectué à l'aide de données anonymisées, si possible, et à défaut codées, à chaque fois que la finalité escomptée peut être atteinte par ce procédé.
- L'accès aux données traitées dans tout autre but légitime est limité à des services ou à des membres du personnel autorisés du Secrétariat général titulaires d'une autorisation d'accès spécifique.

#### Article 134 : La conservation des données

- Les données traitées dans tout autre but légitime sont conservées pour une période strictement nécessaire à la réalisation des finalités pour lesquelles elles sont traitées et n'excédant pas la durée maximale déterminée par le Comité exécutif.
- Cette période peut être prolongée uniquement en cas de conservation de données à des fins historiques ou de traitement anonymisé ou codé des données, à condition que cette prolongation demeure elle-même nécessaire à la réalisation des finalités pour lesquelles les données sont traitées.

**CHAPITRE II :**  
**RÈGLEMENT DES DIFFÉRENDS**

**Article 135 : Règlement des différends**

1. Les différends auxquels les Bureaux centraux nationaux, les entités internationales, les entités nationales, les entités privées ou le Secrétariat général sont parties concernant des décisions relatives à la conformité et qui surviennent dans le cadre de l'application du présent Règlement sont régis par la procédure suivante :
  - a) Les différends sont en principe résolus par voie de concertation. Si celle-ci n'aboutit pas, une décision définitive relative à la conformité est rendue par le Secrétariat général ;
  - b) Après qu'une décision définitive relative à la conformité a été rendue, toute partie au différend peut soumettre au Comité exécutif une question de politique générale découlant dudit différend et relative à l'application ou à l'interprétation du Statut, du Règlement sur le traitement des données ou des résolutions pertinentes de l'Assemblée générale. Si la question de politique générale ne relève pas des prérogatives du Comité exécutif, ou si le Comité exécutif le juge nécessaire, ce dernier transmet la question de politique générale à l'Assemblée générale.
2. Rien n'empêche les entités concernées de résoudre leur désaccord à l'amiable en dehors de cette procédure de règlement des différends.
3. L'Assemblée générale adopte des règles d'application régissant le règlement des différends.

\*\*\*\*\*

## **RÈGLEMENT D'INTERPOL SUR LE TRAITEMENT DES DONNÉES**

---

### **ANNEXE : CHARTE D'ACCÈS AU SYSTÈME D'INFORMATION D'INTERPOL PAR LES ENTITÉS NATIONALES**

La présente charte a pour objectif de formuler clairement les conditions auxquelles les entités nationales peuvent être autorisées par les Bureaux centraux nationaux de leurs pays respectifs, conformément à l'article 21 du Règlement d'INTERPOL sur le traitement des données, à consulter directement des données traitées dans le Système d'information d'INTERPOL ou à fournir directement des données aux fins de traitement dans ledit système.

1. L'accès direct au Système d'information d'INTERPOL est soumis aux conditions suivantes :

- a) l'accès direct au Système d'information d'INTERPOL et son utilisation sont soumis au Règlement d'INTERPOL sur le traitement des données ;
- b) l'entité nationale accepte les dispositions de ce Règlement ainsi que toute procédure mise en place en application dudit Règlement pour permettre l'accès au Système d'information d'INTERPOL et son utilisation, et consent à s'y conformer ;
- c) l'entité nationale désigne un officier de sécurité ainsi qu'un officier délégué à la protection des données et met en place des procédures destinées à assurer de façon permanente le respect du présent Règlement par ses utilisateurs ;
- d) l'entité nationale accepte, en particulier, que le Bureau central national qui l'a autorisée puisse :
  - i. effectuer des contrôles réguliers, à distance ou sur site, sur le traitement par l'entité nationale des données introduites ou consultées dans le Système d'information d'INTERPOL, afin de s'assurer du respect du Règlement par l'entité nationale ;
  - ii. prendre des mesures conservatoires ou correctives à son encontre en cas d'incident de traitement ;
  - iii. mettre fin à l'accès au Système d'information d'INTERPOL qui lui est conféré en cas de non-respect par l'entité nationale de ses obligations au regard dudit Règlement ou de traitement de données non conforme et répété.

- e) l'entité nationale accepte également que le Secrétariat général d'INTERPOL :
  - i. soit chargé de l'administration générale du Système d'information d'INTERPOL et veille au respect des conditions de traitement des données dans les bases de données de l'Organisation ;
  - ii. puisse prendre toute mesure appropriée, dans la limite dudit Règlement, pour mettre fin à tout traitement non conforme de données, y compris de mettre fin à l'accès au Système d'information d'INTERPOL.

2. L'étendue des droits d'accès de l'entité nationale au Système d'information d'INTERPOL est fixée par le Bureau central national conformément au Règlement d'INTERPOL sur le traitement des données.

\*\*\*\*\*