ROYAUME DE BELGIQUE
Service public fédéral
Affaires étrangères,
Commerce extérieur et
Coopération au Développement

Police

ibz Service public fédéral Intérieur

Recommandations de la Task Force par rapport aux nouvelles initiatives des communes pour améliorer le service aux citoyens

Table des matières

Introduction **2**

1. Contexte **3**

2. Types de projets **3**

2.1. Kiosque self-service **3**

2.1.1. Demandes obligatoires au guichet 3

2.1.2. Identification du demandeur 4

2.1.3. Software et hardware du kiosque 5

2.1.4. Responsabilités des administrations communales 5

2.2. Livraison à domicile **6**

2.2.1. Responsabilité contractuelle 6

2.2.2. Documents concernés 7

2.2.3. Protection des données personnelles 7

2.2.4. Traçabilité et statut des passeports 8

2.2.5. Identification du destinataire 9

2.2.6. Sealbag séparé pour les passeports destinés à une livraison à domicile ? 10

2.3. Distributeur automatique **10**

2.3.1. Risques sécuritaires 11

2.3.2. Identification du demandeur 11

2.3.3. Obligations procédurales 11

2.4. Kit mobile **12**

3. Conclusions **12**

Introduction

Autorités compétentes : SPF Intérieur, SPF Affaires étrangères, Office des étrangers.

Destinataires : les communes en Belgique.

Documents concernés : les passeports ordinaires, les titres de voyage pour réfugiés, apatrides ou étrangers, les cartes d'identité et les titres de séjour.

Ayants-droit : citoyens qui introduisent une demande de documents précités dans une commune.

Base réglementaire :

- Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (= règlement RGPD).
- Règlement (UE) 2025/1208 du Parlement européen et du Conseil du 12 juin 2025relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation.
- Loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers.
- Loi du 8 août 1983 organisant un Registre national des personnes physiques, article 8 (MB 21-04-1984).
- Loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour (MB 03-09-1991)
- Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (MB 05-09-2018).
- Code consulaire du 21 décembre 2013, chapitre 10 « Les passeports » (MB 21-01-2014).
- Loi du 10 février 2015 relative au traitement automatisé de données à caractère personnel nécessaires aux passeports et titres de voyage belges (MB 02-03-2015).
- L'arrêté royal du 8 octobre 1981 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers.
- L'arrêté royal du 25 mars 2003 relatif aux cartes d'identité (MB 28-03-2003).
- Note-Cadre Sécurité Intégrale 2026-2029 – point 9.6. de la partie IV.

1. Contexte

La Note-Cadre Sécurité Intégrale 2026-2029 (point 9.6. de la partie IV) souligne, de nouveau, que la lutte contre la fraude à l'identité reste une priorité pour les autorités fédérales. Il y est demandé de continuer la sécurisation des procédures de délivrance en renforçant, entre autres, les aspects réglementaires par rapport à la prévention et la lutte contre la fraude, les aspects sécuritaires dans les communes, etc.

D'autre part, depuis quelques années, plusieurs communes ont contacté les SPF Intérieur et Affaires étrangères afin de leur demander un avis concernant des projets d'innovation en matière de demande et de délivrance de documents d'identité, de voyage et de séjour : kiosque « self enrollment », livraison à domicile, distributeur de documents, kit mobile, etc.

Ces initiatives actuellement développées par les autorités locales pour améliorer le service au client rendent les processus de délivrance de ces documents plus complexes et parfois plus vulnérables à la fraude. En effet, aujourd'hui l'ensemble de ces processus sont pilotés humainement par des fonctionnaires habilités.

L'objectif de ce document est de donner des directives et consignes minimales aux communes par rapport à ces projets d'innovation. La Task Force fraude à l'identité veut s'assurer que de telles initiatives ne vont pas à l'encontre de la sécurité des processus de demande et de délivrance de documents, telle qu'exigé par la Note-Cadre de Sécurité Intégrale 2026-2029.

De plus, puisque les communes en question concluent souvent pour l'exécution de ces projets des contrats avec des firmes privées non agréées par les SPF Intérieur et Affaires étrangères, la Task Force souhaite définir clairement les responsabilités respectives des SPF précités et des communes qui concluent un tel contrat.

Pour faciliter votre lecture, chaque directive est facilement repérable grâce à cette icône :

2. Types de projets

2.1. Kiosque self-service

Certaines communes désirent installer dans leurs locaux des kiosques self-service permettant au citoyen d'y enregistrer sa demande de document sans devoir passer au guichet.

2.1.1. Demandes obligatoires au guichet

Afin de limiter les risques, toutes les demandes ne peuvent être introduites via un kiosque self-service.

Les demandes suivantes devront toujours être introduites au guichet sous contrôle d'un fonctionnaire habilité :

- Toutes les premières demandes d'un document (contrôle automatisé) ;
- Toutes les demandes faisant suite à une perte, un vol ou une destruction d'un document (contrôle automatisé) ;
- Toutes les demandes introduites en procédure urgente ou très urgente ;
- Toutes les demandes qui ne peuvent être finalisées dans le kiosque : problème reconnaissance faciale, signature, empreintes, etc ;
- Toutes les demandes de ressortissants étrangers dont le renouvellement du titre de séjour est soumis à la production de preuves supplémentaires ou nouvelles comme l'attestation de travail ;
- Toutes les demandes de titres de voyage pour réfugiés, apatrides ou étrangers ;
- Toutes les demandes de passeports diplomatiques ou de service[1] ;
- Toutes les demandes de personnes radiées d'office et de personnes résidant à l'étranger (contrôle automatisé) ;
- Toutes demandes de personnes mineures et de personnes sous protection de mesures judiciaires (contrôle automatisé) ;
- Toutes les demandes de personnes ayant été signalées par les autorités policières, judiciaires ou de sécurité et qui se retrouvent soit dans Passban, soit dans eIDban (contrôle automatisé).

2.1.2. Identification du demandeur

Il est indispensable que le demandeur introduisant sa demande via le kiosque soit identifié sans équivoque. A cette fin, il y introduira sa carte d'identité et son code PIN.

Le système doit intégrer un module de reconnaissance faciale[2] pour comparer la photo prise dans le kiosque avec les photos de documents précédents ou un module de comparaison d'empreintes[3] agréé par les SPF concernés. L'utilisation d'un tel module doit être encadré juridiquement et doit garantir une qualité de résultat. Vu les traitements envisagés (reconnaissance faciale et/ou comparaison d'empreintes), conjugué au fait que le traitement concernera une grande quantité d'individus : une DPIA est nécessaire

[1] Les communes ne sont pas compétentes pour enregistrer les demandes de passeports diplomatiques ou de service. Toutefois, le SPF Affaires étrangères peut exceptionnellement leur demander d'agir comme guichet avancé pour enregistrer les données biométriques des demandeurs de ces passeports. Cela ne peut se faire qu'après l'accord préalable du SPF Affaires étrangères et au guichet de la commune.
[2] Comparaison avec les bases de données des photos précédentes (passeports, eID et titres de séjour).
[3] Comparaison "one to one" des empreintes sur la puce du document.

2.1.3. Software et hardware du kiosque

Le software utilisé dans le kiosque doit être reconnu par les autorités fédérales compétentes afin de :

- Uniformiser les différents processus de demande et de délivrance des documents ;
- Sécuriser les accès aux bases de données fédérales contenant les données d'identification à caractère personnel ;
- Garantir la protection des données à caractère personnel ;
- Eviter les attaques externes sur les systèmes informatiques des autorités fédérales ;
- Assurer la disponibilité et la viabilité des systèmes informatiques ;
- Garantir l'interopérabilité des systèmes mis en place dans les différentes communes ;
- Assurer la conformité du système et des procédures avec la réglementation européenne eIDAS afin que l'Etat belge ne perde pas sa qualification comme trust service provider.

Le hardware du kiosque devra être agréé par les autorités fédérales compétentes afin de :

- Garantir la qualité et la sécurité des systèmes utilisés ;
- Garantir l'interopérabilité des systèmes mis en place dans les différentes communes ;
- Eviter les attaques externes sur les systèmes informatiques des autorités fédérales ;
- Garantir une configuration uniforme du hardware dans toutes les communes.

2.1.4. Responsabilités des administrations communales

L'utilisation des kiosques self-service ne peut se faire qu'en présence physique, dans le local où les kiosques sont installés, d'un fonctionnaire communal habilité pour la demande et la délivrance des documents d'identité, de voyage et de séjour. Celui-ci doit pouvoir intervenir en cas de problèmes rencontrés par le citoyen lors de l'enregistrement de sa demande au kiosque.

L'activation des documents d'identité et de séjour doit toujours être effectuée au guichet physique. Sous certaines conditions, la délivrance des passeports pourra se faire sans intervention humaine (voir chapitre 2.3. Distributeur automatique).

La commune décrit les mesures techniques et organisationnelles pour se conformer aux exigences RGPD et pour garantir les droits des personnes concernées, ou encore réalise une DPIA (Data Protection Impact Assessment).

La commune désigne un responsable technique pour les kiosques qui doit être renseigné au SPF Intérieur. Le SPOC communal fraude à l'identité sera le point de contact pour les SPF compétents en cas de suspicion de fraude à l'identité.

2.2. Livraison à domicile

Certaines communes désirent délivrer les documents d'identité, de voyage et de séjour à domicile au citoyen via une société privée. D'autres le font déjà pour les passeports.

Jusqu'à l'apparition de telles initiatives, la centralisation de la délivrance des documents d'identité, de voyage et de séjour visait à diminuer le risque de vol des documents dans les communes. Il ne faudrait pas que le phénomène réapparaisse par l'ajout d'autres méthodes de délivrance moins sécurisées.

Le contrat conclu entre la commune et la société privée doit donc garantir l'intégrité de la chaîne de l'identité dont la délivrance du document n'est que le maillon ultime.

2.2.1. Responsabilité contractuelle

Les SPF Intérieur et Affaires étrangères n'ont aucune relation juridique ou contractuelle avec la société de livraison désignée par la commune et ne peuvent donc tenir cette société responsable en cas de problème (vol, perte, dommage, utilisation abusive de données personnelles, ...). En d'autres termes, nos SPF sont seulement responsables des documents d'identité, de voyage et de séjour jusqu'au moment de leur livraison par la société de production à la commune. En cas de contrat entre la commune et un sous-traitant, il y a lieu de se référer à l'article 28 du Règlement général sur la protection des données (RGPD).

Pour le trajet entre la commune et le citoyen, seule la commune est responsable. Les communes doivent donc régler elles-mêmes cette responsabilité avec leur société de messagerie, car il existe bien une relation juridique et contractuelle entre elles. Les SPF Intérieur et Affaires étrangères conseillent donc aux communes d'inclure dans le contrat avec la société les dispositions nécessaires relatives à la compensation de tout dommage qui résulterait de la livraison à domicile (vol, perte, dommages, usage abusif des données personnelles,...). En outre, il doit stipuler les conditions d'habilitation du personnel chargé du traitement des passeports. Toute forme de sous-traitance par la société privée contractée par la commune est interdite.

Pour ces raisons, certaines informations devraient être transmises au SPF concerné (Affaires étrangères ; voir 2.2.2. ci-après) en temps utiles comme le nom de la société contractée, son siège social, ses coordonnées de contact, la date à laquelle le contrat débuterait et la date d'expiration du contrat. Ces informations peuvent être transmises à la Direction C2 Documents de Voyage et d'Identité du SPF Affaires étrangères : passeport@diplobel.fed.be

2.2.2. Documents concernés

La délivrance des **documents d'identité et de séjour** implique un matching des empreintes digitales du titulaire ainsi qu'une activation éventuelle des certificats sur ces documents. Ces actes ne peuvent en aucun cas être exécutés par une société privée. Ils doivent être effectués par un agent communal habilité.

Dès lors, une livraison à domicile n'est pas envisageable pour ces documents (sauf pour certaines situations spécifiques via stations biométriques).

Par contre, en ce qui concerne **les passeports et titres de voyage**, un matching des empreintes et une activation de certificats n'étant pas encore d'application, un contrat de livraison à domicile pourrait être conclu entre la commune et une société privée sous certaines conditions énumérées dans les chapitres suivants.

Toutefois, la livraison à domicile ne sera pas possible :

- si le passeport précédent n'a pas été remis et annulé à la commune lors de la demande du nouveau passeport ;
- si le SPF Affaires étrangères vous fait savoir, même après l'introduction de la demande, que le passeport ne pourrait pas être délivré sans son accord préalable (suspicion de fraude). Dans ce cas, le demandeur devra se présenter à la commune.

2.2.3. Protection des données personnelles

Lors de la conclusion d'un contrat pour la livraison à domicile, la commune doit se conformer à un certain nombre de conditions juridiques et pratiques concernant le traitement des données personnelles :

- **Données personnelles sensibles sur la puce du passeport :**

  La puce du passeport contient un certain nombre de données personnelles du titulaire:
  - les données personnelles ;
  - les caractéristiques biométriques (photo, empreintes digitales).

  Contrairement aux empreintes digitales, les données personnelles et la photo ne sont pas protégées contre la lecture et le stockage non autorisés. La société de messagerie pourrait donc utiliser un lecteur de passeport et un logiciel associé disponibles dans le commerce pour lire ou conserver les données personnelles et la photo ou, dans le pire des cas, en abuser.

La Task Force recommande donc que les communes prennent les mesures nécessaires pour empêcher que la société puisse avoir directement accès à la puce des passeports qu'elle transporte. Cela peut se faire, par exemple, en livrant les passeports dans une enveloppe scellée, qui n'est pas ouverte par la société, au demandeur.

➢ **Utilisation des données personnelles pour la délivrance du passeport :**

Afin de pouvoir livrer le passeport au demandeur, la société de messagerie devra dans tous les cas traiter et utiliser un minimum de données personnelles. La Task Force vous rappelle que tout traitement de données à caractère personnel est soumis aux dispositions du Règlement RGPD et de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (voir article 2 pour la définition de " traitement de données à caractère personnel ").

La Task Force rappelle aux communes le principe de proportionnalité du traitement des données au regard de la finalité poursuivie et conseille donc aux communes :

- de limiter autant que possible les données personnelles mises à la disposition de la société privée (nom, prénom, adresse, numéro de téléphone, e-mail, ...),
- d'éviter l'utilisation du numéro du registre national,
- et de ne pas permettre à la société de conserver les données plus longtemps que ce qui est strictement nécessaire pour délivrer le passeport au destinataire.

La commune étant le responsable du traitement des données personnelles qu'elle mettrait éventuellement à disposition de la société privée, devra intégrer dans le contrat avec cette société une convention RGPD précisant les données pouvant être utilisées et les modalités de cette utilisation.

2.2.4. Traçabilité et statut des passeports

Un passeport biométrique authentique est un produit très convoité et, s'il tombe entre de mauvaises mains, l'abus n'est pas exclu. C'est pourquoi, les mouvements du passeport doivent toujours être tracés (y compris sur la route entre la commune et le demandeur) et que le statut du passeport doit toujours être à jour et correspondre à la réalité.

Par conséquent, les conditions suivantes sont à respecter :

➢ **Traçabilité sur la route commune-demandeur :**

Pour minimiser les risques de vol, de perte ou d'usage abusif d'un passeport authentique, une parfaite traçabilité du passeport est obligatoire. Jusqu'à la livraison du passeport à la commune, cette traçabilité est garantie par les dispositions du contrat avec le fabricant du passeport. Ce dernier a été audité plusieurs fois en termes de sécurité et de traçabilité et a dû, lorsque cela était jugé nécessaire, adapter ses procédures.

Toute livraison à domicile organisée par la commune ne relève pas des dispositions du contrat « passeports » entre le SPF Affaires étrangères et le producteur des passeports et doit donc être réglée dans le contrat entre la commune et la société de messagerie. Ce dernier doit contenir les **dispositions nécessaires pour garantir la traçabilité** (par exemple via un système

de «track & trace»). Un audit préalable auprès de la société de messagerie sur les mesures qu'ils prendront pour la sécurité et la traçabilité peut aussi être très utile.

- **Adaptation du statut du passeport :**

Il est très important que le statut du passeport soit toujours à jour et corresponde à la réalité, afin d'éviter les abus (même les anciens passeports périmés peuvent encore être utilisés frauduleusement). Par ailleurs, la ***loi du 10-02-2015 relative au traitement automatisé de données à caractère personnel nécessaires aux passeports et titres de voyage belge*** n'autorise pas l'accès à la base de données des passeports – dans laquelle le statut des passeports est enregistré et actualisé - à une entreprise autre que le fabricant du passeport.

Par conséquent, la commune elle-même doit assurer l'adaptation correcte du statut du passeport (p. ex. «délivré», «détruit», «annulé»). **Cela ne peut pas être confié à la société privée**.

- **Récupérer & annuler/détruire le précédent passeport :**

Vu que les anciens passeports périmés peuvent également être victimes d'abus (par exemple, utilisation non autorisée des données sur la puce, utilisation des pages de visa vides pour créer un faux passeport, ...), il est important qu'ils soient physiquement récupérés puis annulés ou détruits **par la commune elle-même**, pas par la société de messagerie.

2.2.5. Identification du destinataire

Lors de la délivrance d'un passeport au guichet de la commune, le fonctionnaire communal peut s'assurer que la personne qui reçoit le passeport est bel et bien le demandeur. Même en cas de retrait par un tiers mandaté par le demandeur, les contrôles nécessaires peuvent avoir lieu au guichet (formulaire de procuration, carte d'identité du tiers, ...).

C'est moins évident dans le cadre d'une livraison à domicile par une société de messagerie. Pour éviter que le passeport ne tombe entre de mauvaises mains, il faut prendre en compte les éléments suivants:

- **Elaboration d'une procédure de délivrance cohérente:**

Le passeport ne peut être délivré qu'au **demandeur lui-même** (vérification de son identité sur la base de sa carte d'identité). S'il s'agit du passeport **d'un mineur**, il vous est demandé de suivre la même procédure qu'au guichet, c'est-à-dire de remettre le passeport à l'un des deux parents conformément aux règles sur l'autorité parentale.

Au cas où le demandeur ne serait pas présent au moment de la livraison à domicile, le colis ne peut **en aucun cas** être livré mais doit être ramené par la société de messagerie. En attendant

une éventuelle deuxième livraison, le passeport doit être conservé dans un lieu sécurisé uniquement accessible au personnel habilité soit de la commune soit de la société privée (voir point 2.2.1. supra).

Il est à recommander **d'intégrer toutes ces procédures de délivrance dans le contrat avec la société de messagerie**. Un audit préalable auprès de la société de messagerie sur les mesures qu'ils prendront pour la sécurité et la traçabilité peut aussi être très utile.

- **Introduction éventuelle d'un contrôle des empreintes digitales comme contrôle d'identité :**

Il n'est pas exclu qu'une comparaison (*matching*) des empreintes digitales du demandeur (= destinataire de la livraison) avec celles sur la puce du passeport délivré soit instaurée à l'avenir. Cela peut être utile d'une part en tant que contrôle de qualité et d'autre part dans le contexte de la lutte contre la fraude à l'identité. Un tel *matching* ne sera probablement pas systématiquement imposé mais ponctuellement en cas de doute.

Ce contrôle est une **compétence exclusive de l'exécutif** (= les autorités publiques) et non d'une société privée. En outre, il existe des objections juridiques et techniques à ce que les empreintes digitales soient lues par une société privée (abus des données biométriques sensibles, les lecteurs de passeports doivent être individuellement certifiés par l'autorité centrale pour pouvoir lire les empreintes digitales, etc.).

Il est en tous cas recommandé, s'il y a le moindre doute sur l'identité du destinataire du passeport, de demander un retrait au guichet!

2.2.6. Sealbag séparé pour les passeports destinés à une livraison à domicile ?

Le producteur des passeports pourrait éventuellement livrer les passeports destinés à la livraison à domicile dans un sealbag séparé à la commune. Cependant, des frais supplémentaires seront facturés pour cela, frais qui ne sont pas couverts par le contrat « passeports » entre le SPF Affaires étrangères et le producteur des passeports.

Les communes intéressées pourront contacter le producteur des passeports afin d'organiser cela et la facturation sera réglée directement entre la commune et le producteur des passeports.

2.3. Distributeur automatique

Certaines communes désirent délivrer les documents d'identité, de voyage et de séjour par un distributeur automatique permettant au citoyen de récupérer son document sans devoir passer au guichet.

Toutefois, les documents susmentionnés sont à considérer comme des documents de très grande valeur comportant des données personnelles particulièrement sensibles. Ils doivent être délivrés dans les meilleures conditions sécuritaires, limitant ainsi les risques d'abus ou de détournement. Dans ce sens, une distribution de documents via un distributeur n'est pas possible pour les raisons suivantes :

2.3.1. Risques sécuritaires

Les risques sécuritaires concernant ce type de distributeur accessible 24h/7j au public sont considérables :

- Attrait ciblé pour les fraudeurs et bandes organisées. Un distributeur situé à l'extérieur du bâtiment, même blindé, sera toujours plus vulnérable au vol ou au hacking.
- Risques pour les citoyens se rendant au distributeur.
- Risques de vandalisme du distributeur.

2.3.2. Identification du demandeur

La délivrance de documents doit se faire dans un environnement sécurisé et sous supervision d'un agent communal. Il doit y avoir un contrôle de l'identité de la personne qui vient chercher le document par l'agent communal (via le Registre national). Un distributeur n'est pas relié au Registre national, à Belpic ou Belpas pour les vérifications nécessaires de l'identité du titulaire.

Il est donc impossible d'identifier avec certitude la personne venant chercher le document.

2.3.3. Obligations procédurales

Pour le retrait des différents documents, il existe des procédures réglementaires à respecter :

- Pour les **passeports** : le statut du passeport doit être adapté quand il est remis à son titulaire (statut « délivré »), ceci afin de garantir une parfaite traçabilité du document. Cela est d'autant plus important lorsqu'une enquête s'impose quand le document serait, pendant son cycle de vie, déclaré « volé » ou « perdu ». Le document remplacé doit en plus être annulé et remis à l'agent communal pour destruction immédiate lors de la remise du nouveau document ;
- Pour les **cartes d'identité et titres de séjour** : le statut du document doit être adapté et les certificats de la carte doivent être activés via Belpic pour permettre de s'identifier en ligne et d'apposer une signature numérique, ceci afin de garantir une parfaite traçabilité du document. Le document remplacé doit être annulé et remis à l'agent communal pour destruction immédiate lors de la remise du nouveau document. Un matching des empreintes digitales doit aussi être effectué au moment de la délivrance de la carte.

2.4. Kit mobile

Certaines communes nous ont fait part de leur souhait d'acheter des kits mobiles pour la demande et la délivrance de documents d'identité, de voyage et de séjour. Le but est de pouvoir enregistrer les demandes de personnes ne pouvant se déplacer à l'administration communale (p.ex. prisonniers, malades, personnes âgées, etc.).

Le SPF Intérieur a développé un kit mobile sous forme de tablette contenant tous les périphériques et logiciels nécessaires pour demander et délivrer des documents d'identité et de séjour ailleurs qu'au guichet de la commune.

Les communes peuvent se procurer le kit mobile auprès de leur fournisseur informatique.

3. Conclusions

Par le biais de ces recommandations, la Task Force ne veut en aucun cas empêcher les communes de conclure des contrats de services avec des sociétés privées afin d'améliorer le service aux citoyens. En effet, c'est aussi l'aspiration des différents SPF représentés dans la Task Force.

Cependant, ces contrats de services doivent répondre à certaines conditions afin de garantir la sécurité des processus de demande et délivrance des documents d'identité, de voyage et de séjour, la protection des données personnelles des citoyens et l'intégrité des bases de données des SPF concernés.

Cela est d'ailleurs dans l'intérêt des communes et de leurs citoyens.

Par conséquent, la Task Force demande aux communes de bien vouloir suivre ces recommandations.