Convention d’utilisation DG SD du SPF BOSA POUR LES SERVICES WEB de l’INTÉGRATEUR DE SERVICES FÉDÉRAL

Objectif du document :

Une convention d’utilisation est un contrat qui stipule les conditions liées à l’utilisation d’un service fourni par une partie à l’autre partie. Il s’agit dans ce cas d’un document formel signé au nom d’une partie (« l’utilisateur ») qui souhaite utiliser les services de la DG SD du SPF BOSA, plus précisément un ou plusieurs services web de l’intégrateur de services fédéral. La convention est signée par une personne qui peut valablement représenter cette partie à cette fin. En signant la convention d’utilisation, l’utilisateur se déclare d’accord avec les conditions générales des services de la DG SD du SPF BOSA : <https://bosa.belgium.be/fr/conditions-generales-services-dg-simplification-et-digitalisation> (voir également annexe). Cette convention décrit plus en détail les conditions d’utilisation spécifiques et les niveaux de service.

SPF STRATÉGIE ET APPUI - DG Simplification et Digitalisation

Version : 6.3 Final, 25/11/2023

TABLE DES MATIÈRES

[1. Conditions spécifiques 3](#_Toc1195710715)

[1.1 Description du service 3](#_Toc1690968434)

[1.2 Utilisation du service 4](#_Toc958700021)

[1.3 Rôles et responsabilités 5](#_Toc1707463542)

[1.4 Coûts liés à l’utilisation du service 7](#_Toc782009449)

[Sécurisation de la FSP de la DG SD du SPF BOSA 7](#_Toc903259375)

[Sécurisation de l’utilisateur 7](#_Toc556253779)

[Finalité 8](#_Toc390375355)

[Audit trail 8](#_Toc431830314)

[2. Niveaux de service 9](#_Toc1990119616)

[2.1 Disponibilité du service 9](#_Toc1812723604)

[2.2 Capacité et performance 11](#_Toc1665035060)

[2.3 Niveaux de service 11](#_Toc678496737)

[2.4 Support 11](#_Toc811439367)

[2.5 Rapports et réunions de service 17](#_Toc1289477529)

[3. Parties et signature 18](#_Toc1821018529)

# Conditions spécifiques

## Description du service

Par le biais de la DG SD du SPF BOSA, les utilisateurs (administrations ou entités qui consomment les services offerts par le SPF BOSA) peuvent recevoir des données provenant de banques de données qui sont rendues accessibles par la DG SD du SPF BOSA en tant qu’intégrateur de services fédéral. La DG SD du SPF BOSA a pour but de mettre des données provenant de banques de données (qu’il s’agisse ou non de sources authentiques) à la disposition d’utilisateurs de manière intégrée. Cela s’inscrit dans la mission de la DG SD du SPF BOSA en tant qu’intégrateur de services fédéral conformément à la loi du 15 août 2012 relative à la création et à l’organisation d’un intégrateur de services fédéral.

Concrètement, la DG SD du SPF BOSA met à la disposition des utilisateurs une plateforme (Federal Service Platform, ci-après « FSP ») permettant la consultation ou la communication électronique standardisée de données, d’une application à l’autre.

La FSP comprend différents services web qui permettent aux utilisateurs d’accéder à des données intégrées ou non provenant d’une ou de plusieurs banques de données qui appartiennent à des services publics ou des instances chargées d’une mission d’intérêt public.

Les instances auxquelles les banques de données appartiennent sont également appelées *service providers*.

Les utilisateurs qui ont accès aux données sont également appelés *service consumers*.

Les services web sont regroupés en *webservice families*. Une *webservice family* est un ensemble logique de services web. Une *webservice family* est constituée de services web liés entre eux par leur contenu fonctionnel et/ou par la banque de données.

Dans le cadre de ces services, la DG SD du SPF BOSA se charge des aspects suivants :

* *la mise à disposition de la FSP de manière standardisée, y compris les mises à jour*
* *la gestion opérationnelle, la sécurisation et la gouvernance de la FSP*
* *la publication d’un catalogue de services web et des informations techniques afin d’accéder à ces services*
* *le support dans le cadre du calibrage et de l’utilisation des services web*

## Utilisation du service

Pour pouvoir utiliser les services, l’utilisateur introduira une demande auprès du Service Desk de la DG SD du SPF BOSA.

Conformément à la réglementation applicable, l’utilisateur est tenu de soumettre :

- une base juridique valable (autorisation/protocole/délibération) s’il s’agit d’une demande de consultation ou de communication de données à caractère personnel ;

- et, pour tous les types de données, une autorisation de l’instance qui gère la banque de données.

Pour une demande de consultation ou de communication de données provenant de certaines banques de données, comme le Registre national et le Registre Bis, vous devez disposer d’une autorisation de l’instance compétente (le cas échéant, une délibération de l’ancien Comité sectoriel du Registre national, une délibération du Comité de la sécurité de l’information (« CSI ») ou une autorisation du ministre qui a l’Intérieur dans ses attributions). Pour les autres données à caractère personnel, un protocole[[1]](#footnote-1), une délibération d’un ancien Comité sectoriel ou une délibération du CSI peuvent être soumis.

Si vous n’en disposez pas, la banque de données peut refuser votre autorisation d’accès.

Si, pour quelque raison que ce soit, la validité de la base juridique soumise (autorisation/protocole/ délibération) prend fin, l’utilisateur doit, de sa propre initiative, en informer immédiatement la DG SD du SPF BOSA et l’instance qui gère la banque de données et l’utilisateur doit, de sa propre initiative, cesser immédiatement d’utiliser les services concernés de la DG SD du SPF BOSA en tant qu’intégrateur de services fédéral.

Outre la présente convention d’utilisation conclue pour l’utilisation de la FSP, une annexe à la présente convention d’utilisation est jointe et signée pour chaque service web pour une finalité déterminée. L’annexe mentionnera le service web, la finalité pour laquelle les données seront traitées, l’autorisation/le protocole/la délibération pertinent(e) et l’autorisation d’accès à la banque de données et l’avis des DPOs concernés.

La connexion au service sera préparée sur la base des données de configuration. Après les tests d’intégration, le service passera en production.

## Rôles et responsabilités

Les responsables des banques de données sont chacun responsables du traitement au sens de l’art. 4, 7°, du RÈGLEMENT (UE) 2016/679 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 (« RGPD ») pour les données dans leur propre banque de données. Ils sont responsables de l’organisation des processus de manière transparente pour faire en sorte que les données soient aussi complètes, exactes, précises et actualisées que possible. Ils sont responsables de la collecte des données dans la banque de données, de l’enregistrement des données avec des garanties de qualité et de disponibilité, et de la décision de mise à disposition ou non via l’intégrateur de services. Les responsables des banques de données effectuent le traitement dans le cadre juridique applicable à la banque de données et conformément à celui-ci.

Si les utilisateurs doutent de l’exactitude des données dans la banque de données, ils ont le droit de le signaler à la DG SD du SPF BOSA ou aux responsables de la banque de données. La banque de données est alors tenue d’analyser sérieusement la notification et, le cas échéant, d’apporter les corrections nécessaires.

En tant qu’intégrateur de services, la DG SD du SPF BOSA agit en qualité de responsable du traitement au sens de l’art. 4, 7°, du RGPD. La DG SD du SPF BOSA est à cet égard responsable des traitements consistant à rendre accessibles les données des banques de données selon les règles des banques de données, à les transmettre à la demande de l’utilisateur, à les intégrer à partir de différentes banques de données selon les règles des banques de données et à transmettre les données intégrées à la demande de l’utilisateur. La DG SD du SPF BOSA effectue le traitement dans le cadre de la loi du 15 août 2012 relative à la création et à l’organisation d’un intégrateur de services fédéral.

La DG SD du SPF BOSA rend accessibles et traite les données de la banque de données à la demande de l’utilisateur ou de l’instance qui gère la banque de données. Le responsable de la banque de données détermine les règles auxquelles l’utilisateur doit répondre avant de pouvoir recevoir la communication des données concernées via la DG SD du SPF BOSA. La DG SD du SPF BOSA s’engage à ne pas communiquer de données aux utilisateurs qui ne respectent pas les règles. La DG SD du SPF BOSA doit pouvoir démontrer à tout moment le respect de ces règles.

La DG SD du SPF BOSA s’engage à examiner, pour chaque demande de consultation et de communication, si l’utilisateur demandeur et la demande en question respectent les règles spécifiques déterminées par le responsable de la banque de données auprès de la DG SD du SPF BOSA.

En tant que destinataire des services fournis par la DG SD du SPF BOSA, l’utilisateur agit en qualité de responsable du traitement au sens de l’art. 4, 7°, du RGPD, c’est-à-dire la personne qui, seule ou avec d’autres, détermine la finalité et les moyens du traitement des données à caractère personnel. L’utilisateur est à cet égard responsable des données reçues et de leur traitement conformément à l’autorisation/au protocole/à la délibération dont il dispose et conformément à la législation applicable. Cela signifie notamment que les mesures nécessaires seront prises pour garantir que seules les personnes compétentes peuvent prendre connaissance des données ou les utiliser, que les données ne peuvent être utilisées qu’aux fins préétablies et que le principe de proportionnalité doit être respecté.

La DG SD du SPF BOSA et l’utilisateur se prêtent mutuellement assistance afin de s’acquitter de leur obligation de donner suite aux demandes dont les personnes concernées les saisissent en vue d’exercer leurs droits et afin de garantir le respect des obligations prévues aux articles 32 à 36 du RGPD.

La DG SD du SPF BOSA et l’utilisateur tiennent un registre des activités de traitement. Sur simple demande, ils sont tenus de présenter ce registre à l’autorité de contrôle compétente.

Si la DG SD du SPF BOSA ou l’utilisateur ont connaissance d’une violation en rapport avec les données à caractère personnel mises à disposition, ils s’informeront mutuellement dans les meilleurs délais.

La DG SD du SPF BOSA et l’utilisateur s’engagent à respecter le RGPD et toute autre législation pertinente en matière de traitement des données.

La DG SD du SPF BOSA et l’utilisateur s’engagent à informer les personnes agissant sous son autorité des dispositions du RGPD et de ses arrêtés d’exécution, ainsi que de toute prescription pertinente relative à la protection de la vie privée à l’égard du traitement des données à caractère personnel.

Les deux parties ont désigné un délégué à la protection des données et disposent d’une politique et d’un plan de sécurité actuels qui sont révisés annuellement.

Les parties s’échangent l’identité et les données de contact des délégués à la protection des données. Chaque partie informe l’autre partie en cas de changements en la matière.

Les deux parties s’engagent à prendre les mesures techniques et organisationnelles nécessaires pour protéger les données contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l’accès et tout autre traitement non autorisé de données.

Les deux parties s’engagent à documenter toutes les mesures et à les mettre à disposition sur demande aux autres parties et à l’autorité compétente.

## Coûts liés à l’utilisation du service

L’utilisation des services offerts par la DG SD du SPF BOSA est gratuite. Cependant, des frais peuvent éventuellement être imputés par le service auquel ou l’instance à laquelle la source authentique appartient (c’est par exemple le cas pour le Registre national – plus d’infos sur le site web du SPF Intérieur : <https://www.ibz.rrn.fgov.be/fr/registre-national/tarifs/securite>)

### Sécurisation de la FSP de la DG SD du SPF BOSA

La DG SD du SPF BOSA assure une sécurisation optimale de l’accès à la FSP et aux différents service providers.

L’accès à la FSP est configuré après un contrôle détaillé de la demande reçue, qui répond aux conditions suivantes :

1. Convention d’utilisation signée
2. Une copie de la base juridique (autorisation/protocole/délibération)
3. Une copie de l’autorisation de l’instance qui gère la banque de données pour le ou les services pour lesquels cela est requis (voir les informations relatives aux services dans le portefeuille de l’intégrateur de services fédéral : <https://dtservices.bosa.be/fr/services/service-integrator-fsb/catalogue-service-integrator>)
4. Un ou des flux de firewall spécifiques ouverts en fonction du ou des services demandés
5. Disposer d’un certificat SSL FSP

Au niveau de l’application, un certificat ou oAuth Credential est utilisé selon la politique de sécurité appartenant au service.

* Pour le certificat, le CN (Common Name) est l’identifiant unique de l’application du *service consumer*.
* Pour l’oAuth Credential, le ClientID est l’identifiant unique de l’application du *service consumer*.
* Un certificat ou oAuth2 Credential existant ne peut être utilisé pour une deuxième connexion FSP ou plus que moyennant le consentement écrit préalable de la DG SD du SPF BOSA.

### Sécurisation de l’utilisateur

La DG SD du SPF BOSA règle via la FSP la sécurité de la connexion de l’application de l’utilisateur à la source authentique.

La sécurité et le contrôle d’accès des utilisateurs finaux doivent être assurés par l’utilisateur.L’utilisateur se charge de bien sécuriser sa propre application et de mettre en place un système d’authentification des utilisateurs finaux.

En tant qu’élément de guidance sur la sécurité de l’information, FISP peut être utilisé :

: [Politique fédérale sur la sécurité de l'information (FISP) | BOSA (belgium.be)](https://bosa.belgium.be/fr/themes/administration-numerique/strategie-et-politique-du-numerique/politique-federale-sur-la).

L’utilisateur est conscient qu’il a peut-être affaire à des données à caractère personnel ou d’autres catégories de données confidentielles, ce qui l’oblige à prendre les mesures nécessaires et à respecter la législation applicable.

Dans ce cadre, il ne peut notamment pas transmettre ces données à des tiers sans autorisation spécifique.

### Finalité

L’utilisateur soumet par service web une autorisation/un protocole/une délibération dans un but précis et s’engage dès lors à ne faire usage que d’un accès bien précis dans le but spécifique lié à cet accès et tant que l’autorisation/le protocole/la délibération est valide.

### Audit trail

L’utilisateur et la DG SD du SPF BOSA reconnaissent que la mise en place d’un *audit trail* est nécessaire dans le cadre de la prestation de services. Cet *audit trail* assure que les transactions effectuées via l’intégrateur de services de la DG SD du SPF BOSA peuvent être reconstituées afin de respecter l’obligation légale de sécuriser suffisamment les données traitées.

L’utilisateur et la DG SD du SPF BOSA reconnaissent que le principe des « cercles de confiance » (*circles of trust*) s’appliquera à la prestation de services. À cette fin, chaque partenaire de la chaîne sera tenu à titre individuel de prendre les mesures nécessaires pour conserver des données sélectionnées dans son *audit log*, de manière à ce qu’il soit possible, par la combinaison des données tenues à jour par les différents partenaires de la chaîne, de parvenir à une reconstitution complète de l’ensemble du flux de données d’une transaction spécifique.

L’utilisateur et la DG SD du SPF BOSA reconnaissent que, pour ladite reconstitution, d’autres partenaires de la chaîne dépendent des données qu’ils tiennent eux-mêmes à jour.

Dans le cadre d’un *audit trail*, le *service consumer* indique, pour un *messageID* et *timestamp* FSP fourni par la DG SD du SPF BOSA, qui est l’utilisateur final qui a lancé cette requête. Ces données doivent rester disponibles pendant une période de 10 ans. Ces données doivent pouvoir être fournies sur demande par l’utilisateur dans les 24 heures.

L’utilisateur et la DG SD du SPF BOSA sont chacun responsables des procédures et de l’infrastructure leur permettant de répondre à ces exigences de manière sécurisée et dans le respect de la vie privée.

La DG SD du SPF BOSA supprime toutes les données à caractère personnel au terme de la prestation de services relatifs au traitement, à l’exception des audit trails qui sont conservés à la lumière de la réglementation applicable.

# Niveaux de service

## 2.1 Disponibilité du service

* Valeur cible dans l’environnement de production

Pour la FSP proprement dite, un SLA a été conclu avec le prestataire de services de la DG SD du BOSA afin de garantir une disponibilité élevée de la plateforme.

99,95 % pendant les heures d’activité et 99,5 % en dehors de ces heures.

Les heures d’activité s’étendent de 8h30 à 17h en semaine, sauf les jours fériés officiels.

La disponibilité des services web sur la FSP dépend cependant aussi du SLA conclu avec le responsable de la banque de données.

La DG SD BOSA utilisera tous les moyens raisonnables pour garantir une disponibilité aussi élevée que possible des services web.

* FSP dans l’environnement de production

La FSP dans l’environnement de production est en principe disponible 24 heures sur 24 et 7 jours sur 7 (sauf fenêtres de maintenance planifiées). La fenêtre de support s’étend cependant de 8h30 à 17h en semaine (sauf jours fériés).

* FSP dans l’environnement d’intégration

Le service web dans l’environnement d’intégration est en principe disponible 24 heures sur 24 et 7 jours sur 7 (sauf fenêtres de maintenance planifiées). La fenêtre de support s’étend cependant de 8h30 à 17h en semaine (sauf jours fériés).

* Tests dans l’environnement d’intégration

Pour la réalisation de tests étendus dans l’environnement d’intégration, le *service consumer* demandera une fenêtre de test au *service management* de la DG SD du SPF BOSA, sur présentation du plan de test. Cette procédure permet d’éviter toute interférence avec d’autres tests et travaux de maintenance planifiés.

**Procédure de réservation** : e-mail à [FSP@bosa.fgov.be](mailto:FSP@bosa.fgov.be), en mentionnant le numéro de téléphone du demandeur + le type de tests à réaliser.

Procédure de release DG SD du SPF BOSA prévoit jusqu’à 3 versions par service web au même moment à condition de pouvoir garantir une rétrocompatibilité avec la dernière version. Les versions v-1 et v-2 du service web ont toutefois une date d’expiration. Elles resteront disponibles maximum 2 ans avant de disparaître de la plateforme FSP.

L’utilisateur s’engage à suivre le planning de release de la DG SD du SPF BOSA et, si nécessaire, à passer à une nouvelle version, et donc aussi à refaire les tests et à prévoir les moyens nécessaires à cette fin, en cas d’installation d’une quatrième version.

Le nombre de nouvelles versions (avec impact) par an sera limité à 4 maximum.

Le *release* d’un changement ayant un impact sur le *service consumer* comprend 3 étapes :

* communication au sujet du planning du changement (conformément à la matrice ci-dessous) ;
* le changement est mis à disposition dans l’environnement d’intégration (période de transition) ;
* le changement est mis en production.
* Documentation et gestion des versions

La documentation de chaque version d’un service web présent dans l’environnement d’intégration ou de production FSP peut être librement consultée sur : [http://dtservices.bosa.be/fr/services/fsb/catalogue](http://dtservices.bosa.be/fr/serv ices/fsb/catalogue)

* *Matrice de changement*

| **Type de changement** | **Changement majeur** |
| --- | --- |
| Change backwards compatible | 4 semaines à l’avance |
| Change non backwards compatible | 2-6 mois à l’avance (en fonction du fournisseur) |

Des certificats et/ou oAuth2 Credentials sont utilisés dans l’environnement FSP :

* Remplacement du certificat de l’utilisateur

Le *service consumer* est responsable du suivi des certificats qu’il utilise. Il informera la DG SD du SPF BOSA au moins 2 semaines à l’avance de la nécessité de remplacer un certificat. Pour des raisons de sécurité, la prolongation du certificat n’est pas autorisée.

La validité des certificats des utilisateurs dépend du choix de sécurité de la DG SD du SPF BOSA. Actuellement, ils sont valables maximum 12 mois.

* Renouvellement du certificat SSL FSP

Le certificat FSP est renouvelé une fois par an. Les utilisateurs et responsables des banques de données recevront au moins 2 semaines à l’avance ce nouveau certificat et seront avertis, dans les mêmes délais, du moment exact de ce renouvellement.

Le certificat SSL FSP est d’abord remplacé dans l’environnement INT et au moins une semaine plus tard dans l’environnement PROD.

## 2.2 Capacité et performance

* Valeur cible

Pour la plateforme FSP proprement dite, un SLA a été conclu avec le prestataire de services de la DG SD du SPF BOSA afin de garantir une performance élevée de la plateforme.

La capacité et la performance des services web sur la FSP dépendent cependant aussi du SLA conclu avec la banque de données.

La DG SD du SPF BOSA utilisera tous les moyens raisonnables pour garantir une performance aussi élevée que possible des services web.

* Utilisation des ressources

À la demande du *service provider*, il est possible d’imposer sur la FSP un nombre maximum de messages que l’utilisateur peut envoyer à la banque de données par unité de temps.

* Gestion de la capacité

Dans le cadre de la gestion de la capacité de la DG SD du SPF BOSA, l’utilisateur informera la DG SD du SPF BOSA de toute modification au volume initialement prévu qui est généré par l’utilisateur.

## 2.3 Niveaux de service

Les niveaux de service peuvent être consultés dans des SLA prévus individuellement (par *webservice family*) à condition que la DG SD du SPF BOSA dispose d’un SLA avec le *service provider*.

## 2.4 Support

* Flux des incidents

L’ensemble des incidents et demandes sont d’abord notifiés par e-mail ou téléphone au Service Desk de la DG SD du SPF BOSA (voir tableau de contact plus bas), qui transférera les appels aux personnes ou services adéquats au sein de la DG SD du SPF BOSA.

* Priorités des incidents :

|  |  |
| --- | --- |
|  | **Description et critères** |
| **Priorité 1** | **Incident majeur** **(*Major Incident*)** – impact important sur le processus de travail. Le service est indisponible pour tous les utilisateurs.  Blocage du service ou erreur de fonctionnement du service touchant tous les utilisateurs ; la forte diminution de la performance rend le service inutilisable. Aucune solution de contournement (*workaround*) pour les activités n’est disponible.  Divulgation ou compromission ponctuelle de données à caractère personnel (20 individus ou plus concernés) |
| **Priorité 2** | **Priorité élevée** **(*High Priority*)** – Incident bloquant ou grave.  Incidents ayant un impact sensible sur une partie du service. Aucune solution de contournement (*workaround*) pour les activités n’est disponible.  Divulgation ou compromission ponctuelle de données à caractère personnel (moins de 20 individus concernés) |
| **Priorité 3** | **Priorité moyenne (*Medium Priority*)** – Incident sans gravité et sans impact sur les fonctions opérationnelles du service.  Le service ne fonctionne pas conformément aux spécifications mais l’impact sur les activités est minime ou une solution de contournement (*workaround*) utilisable est disponible. Tous les incidents relatifs aux activités qui ne sont pas une P1 ou P2 ou qui ne concernent pas un seul utilisateur. |
| **Priorité 4** | **Priorité normale (*Normal Priority*)** – Incident mineur ou requête de service, impact sur un seul utilisateur des activités.  Pas d’impact sur les activités ou problème fonctionnel mineur. Tous les tickets relatifs à des requêtes ou des plaintes ayant trait aux activités. |
| **Priorité 5** | **Priorité faible** **(*Low Priority*)** – Requêtes, questions ou service pour un seul utilisateur final.  Tous les incidents ou requêtes de service des citoyens (pas d’impact sur les activités). |

* Matrice des priorités :

**Matrice d’urgence/d’impact pour les décisions relatives à la priorité accordée aux incidents en cas de doute :**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Matrice des priorités** | | **IMPACT SUR LES ACTIVITÉS** | | | |
| **Critique (*Critical*)** | **Sérieux (*Serious*)** | **Moyen (*Medium*)** | **Faible (*Low*)** |
| **URGENCE** | **Critique (*Critical*)** | priorité1 | priorité1 | priorité2 | priorité2 |
| **Élevée (*High*)** | priorité1 | priorité2 | priorité2 | priorité2 |
| **Moyenne (*Medium*)** | priorité2 | priorité2 | priorité3 | priorité3 |
| **Faible (*Low*)** | priorité2 | priorité2 | priorité3 | priorité4 |
| **Requêtes (*Requests*)** | priorité4 | priorité4 | priorité5 | priorité5 |

**Définitions de l’impact sur les activités :**

**Critique** **(*Critical*)** – Impact sur un département tout entier ou délai de livraison/service critique ou impact élevé sur les activités sans solution de contournement (*workaround*) possible pour les activités

* **Sérieux** **(*Serious*)** – Impact sur un grand groupe d’utilisateurs ou impact moyen sur les activités sans solution de contournement (*workaround*) possible pour les activités
* **Moyen** **(*Medium*)** – Impact sur un groupe spécifique ou plusieurs utilisateurs, faible impact sur les activités
* **Faible** **(*Low*)** – Impact sur un seul utilisateur

**Définitions de l’urgence :**

* **Critique** **(*Critical*)** – Incident majeur à traiter en priorité, en situation de gestion de crise
* **Élevée** **(*High*)** – Incident très urgent à traiter le plus rapidement possible
* **Moyenne** **(*Medium*)** – Incident urgent à traiter rapidement
* **Faible** **(*Low*)** – Incident non urgent
* **Requêtes** **(*Requests*)** – Demande d’information non urgente
* Délais de réaction :
  + La journalisation et le transfert de l’appel interviennent dans les 30 minutes.
  + Le feed-back des incidents intervient :
    - toutes les 2 heures de travail pour les incidents de classe 1
    - toutes les 4 heures de travail pour les incidents de classe 2
    - toutes les 12 heures de travail pour les incidents de classe 3
  + La remontée de l’incident vers le *service manager* intervient, si l’incident n’est pas encore résolu :
    - après 5 heures de travail pour les incidents de classe 1
    - après 12 heures de travail pour les incidents de classe 2
    - après 1 semaine pour les incidents de classe 3
  + L’e-mail initial du service web est journalisé et transféré dans un délai de 4 heures.
* Personnes de contact (exemple de tableau relatif aux personnes de contact)

| **Type de contact** | **Contact DG SD du SPF BOSA**  *(nom-fonction/tél.-GSM/e-mail/disponibilité)* | **Contact service consumer**  *(nom-fonction/tél.-GSM/e-mail/disponibilité)* |
| --- | --- | --- |
| Single point of contact (SPOC) | Service Desk de la DG SD du SPF BOSA  *Par e-mail :* [*FSB@bosa.fgov.be*](mailto:FSB@bosa.fgov.be)  *Par téléphone entre 8h30 et 17h les jours ouvrables de l’Administration fédérale :* 02 740 79 94 (FR) 02 740 79 93 (NL) |  |
| Notification des incidents/questions | Service Desk de la DG SD du SPF BOSA |  |
| Notification des changements/maintenance | Service Desk de la DG SD du SPF BOSA |  |
| Escalade | Service Manager DIS  Par e-mail : [dis.servicemanagement@bosa.fgov.be](mailto:dis.servicemanagement@bosa.fgov.be)  Par téléphone : voir signatures dans les e-mails |  |
| Remplaçant Escalade | Service Support DIS  *Par e-mail :* [*FSB@bosa.fgov.be*](mailto:FSB@bosa.fgov.be) |  |
| Escalade + 1 | Domain Service Manager DIS |  |
| DPO | Délégué à la protection des données  Par e-mail : [dpo@bosa.fgov.be](mailto:dpo@bosa.fgov.be) |  |
| Statistiques d’utilisation | Service Manager DIS |  |
| Réunion de service | Service Manager DIS |  |

## 2.5 Rapports et réunions de service

S’il le souhaite, le *service consumer* peut utiliser l’outil Service Management Reporting de la DG SD du SPF BOSA. Ces rapports fournissent les statistiques d’utilisation du *service consumer* d’hier à 13 mois dans le passé.

Par ailleurs, des réunions de service sont prévues pour assurer le suivi des niveaux de service, parcourir les incidents majeurs et discuter des anciens et nouveaux changements. La fréquence de ces réunions sera convenue de commun accord entre la DG SD du SPF BOSA et le *service consumer*.

# Parties et signature

Le service est offert à l’utilisateur par la Direction générale Simplification et Digitalisation du Service public fédéral Stratégie et Appui (« DG SD du SPF BOSA »).

L'utilisation du service est soumise aux conditions générales, à la présente convention d'utilisation, en ce compris le Service Level Agreement (SLA), ainsi qu'aux directives techniques et autres de la DG SD du SPF BOSA concernant le service.

En signant la présente convention d’utilisation, l’utilisateur se déclare d’accord avec les conditions générales relatives aux services de la DG SD du SPF BOSA.

Signé le : date :

L’utilisateur :

Nom, fonction du représentant de l’utilisateur :

Signature

**Annexe 1:** Conditions générales relatives aux services de la DG SD du SPF BOSA. La version la plus récente est disponible à l’adresse suivante : <https://bosa.belgium.be/fr/conditions-generales-services-dg-simplification-et-digitalisation>

**Annexe 2**

Remarque :

La convention d'utilisation stipule ce qui suit au point 1.2 Utilisation du service (p4)

En plus de la présente convention d'utilisation conclue pour l'utilisation du PSF, pour chaque service web à finalité spécifique, une annexe sera jointe à la présente convention d'utilisation et signée. L'annexe précise le service web, la finalité du traitement des données, l'autorisation, le protocole, la consultation et l'autorisation d'accès à la base de données.

Nomination :

Afin de faciliter la signature de la dernière version de la convention d'utilisation, le Service Management de l'intégrateur de services fédéraux a décidé que cette information ne sera pas encore ajoutée et obligatoire au présent contrat.

Le Service Management de l'Intégrateur de Services Fédéraux contactera ultérieurement chaque institution pour compléter ces informations.

Aperçu des services web utilisés :

1. Un protocole au sens de l’article 20 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel. [↑](#footnote-ref-1)