|  |  |
| --- | --- |
|  | CONVENTION D’UTILISATION  Federal Trust Services |

**Objectif du document :**

Une convention d'utilisation est un contrat spécifique à un service qui stipule les conditions liées à l'utilisation d'un service spécifique de la DG Transformation digitale du SPF BOSA. Il s’agit d’un document formel signé par les responsables des parties qui souhaitent utiliser le service (« utilisateurs »).

En signant la présente convention d'utilisation, l'utilisateur se déclare d'accord avec [les conditions générales relatives aux services de la DG Transformation digitale du SPF BOSA](https://dt.bosa.be/nl/algemene_voorwaarden_diensten_dg_digitale_transformatie).

**Version :**1.0

**Date :** 11/02/2022

Contenu

[1. Conditions spécifiques 4](#_Toc95476699)

[1.1. Description et fonctionnement du service 4](#_Toc95476700)

[1.1.1. Objet de la présente convention 4](#_Toc95476701)

[1.1.2. Fonctionnement du service 4](#_Toc95476702)

[1.2.Utilisation du service 8](#_Toc95476703)

[1.2.1. Conditions d’utilisation du service 8](#_Toc95476704)

[1.2.2. Rôles et responsabilités liés à l’utilisateur 8](#_Toc95476705)

[1.2.3. Traitement de données à caractère personnel 9](#_Toc95476706)

[1.3 Sécurité 13](#_Toc95476707)

[1.3.1. Sécurisation par l'utilisateur 13](#_Toc95476708)

[1.3.2. Piste d’audit 14](#_Toc95476709)

[2. Niveaux de service 14](#_Toc95476710)

[2.1. Disponibilité et performance 14](#_Toc95476711)

[2.1.1. Disponibilité et performance du service 14](#_Toc95476712)

[2.1.2. Interruption de service planifiée 15](#_Toc95476713)

[2.1.3. Indisponibilité non planifiée (incident) 15](#_Toc95476714)

[2.2. Support 15](#_Toc95476715)

[2.2.1. Support pour l’utilisateur final (première ligne) 15](#_Toc95476716)

[2.2.2. Support supplémentaire (deuxième ligne) 15](#_Toc95476717)

[2.2.3. Escalade des incidents 17](#_Toc95476718)

[2.2.4. Délégué à la protection des données 17](#_Toc95476719)

[2.3. Gestion des modifications 17](#_Toc95476720)

[2.3.1. Mises à jour planifiées 17](#_Toc95476721)

[2.3.2. Demandes des utilisateurs 18](#_Toc95476722)

[2.4. Composantes du service 18](#_Toc95476723)

[2.5. Information, rapports et évaluation 19](#_Toc95476724)

[2.5.1. Information 19](#_Toc95476725)

[2.5.2. Monitoring 20](#_Toc95476726)

[2.5.3. Rapports 20](#_Toc95476727)

[2.6. Gouvernance 20](#_Toc95476728)

[2.6.1. FTS User Board 20](#_Toc95476729)

[2.6.2. Service meeting avec l’utilisateur 20](#_Toc95476730)

[3. Parties et signature 21](#_Toc95476731)

[Annexes 22](#_Toc95476732)

[Conditions générales des services de la DG TD du SPF BOSA 22](#_Toc95476733)

[Informations techniques 22](#_Toc95476734)

# 1. Conditions spécifiques

## Description et fonctionnement du service

### 1.1.1. Objet de la présente convention

« Federal Trust Services (FTS) » est un service offert par la DG Transformation digitale du Service public fédéral Stratégie et Appui (DG TD du SPF BOSA). FTS est un service qui permet aux utilisateurs d'intégrer de manière simple et fiable des signatures, cachets et horodatages électroniques.

Les utilisateurs sont des instances publiques, des instances chargées de missions par des instances publiques et des instances ayant une mission d’intérêt public. L’utilisateur reconnaît appartenir à l’une de ces catégories d’instances.

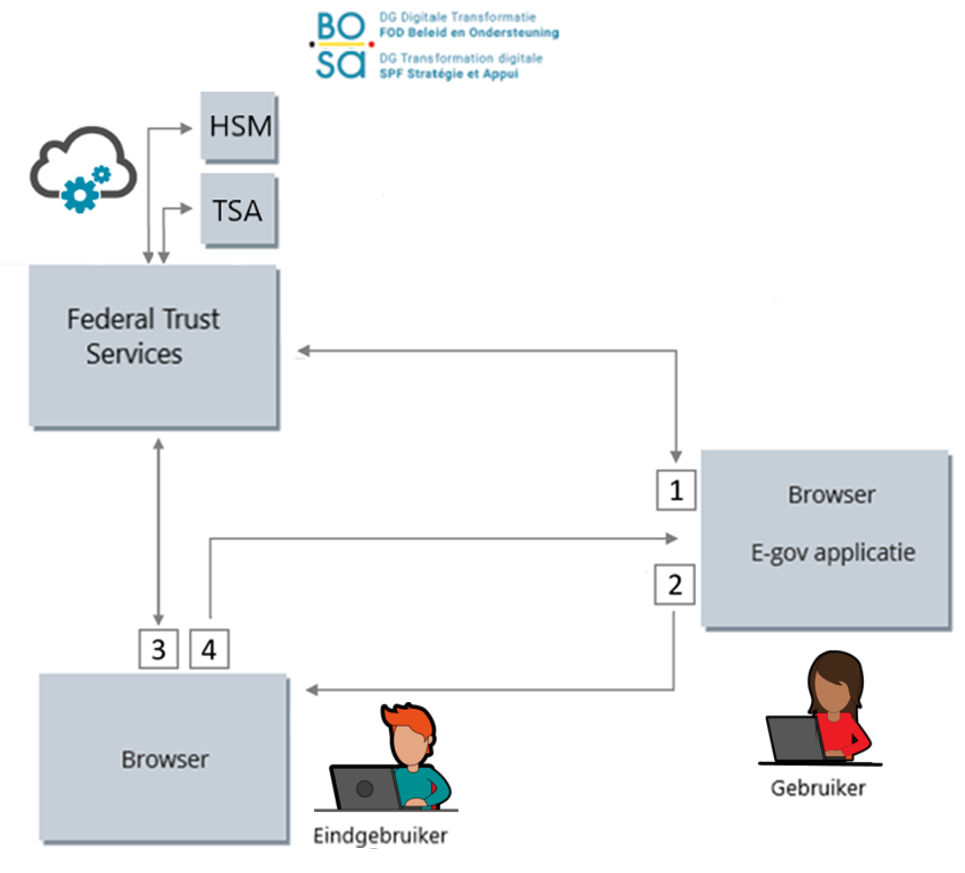
### 1.1.2. Fonctionnement du service

FTS est un module numérique qu’un utilisateur peut intégrer dans ses propres processus numériques. FTS a pour « tâche » délimitée de signer, d'apposer un cachet ou d'horodater des données ou des documents de manière numérique, de façon sûre et simple. L’utilisateur détermine lui-même où et quand FTS intervient et comment les données ou documents signés sont suivis et utilisés.

Le service prévoit l’identification sécurisée (chargement) des données ou documents à signer, la définition de la signature souhaitée, le lancement du processus de signature avec le signataire, la signature effective des données ou des documents avec l’eID/une carte d’étranger et enfin, la réception des données ou des documents signés par voie numérique.

FTS permet également d’apposer des cachets et des horodatages numériques sur des données ou des documents.

*eSignature*

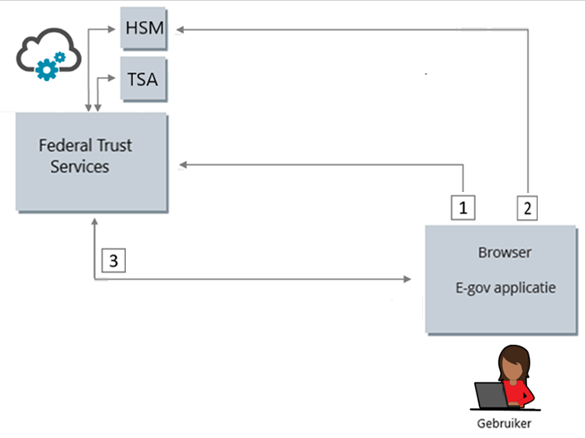


FTS permet à l'utilisateur de fournir une signature numérique qualifiée sans authentification préalable, en utilisant la carte d'identité électronique ou la carte d'étranger[[1]](#footnote-2). FTS prend en charge les formats de signature définis dans les normes et standards européens, y compris les variantes LTA qui nécessitent un ou plusieurs horodatages. Pour plus de détails sur les formats de signature et leurs différences, nous renvoyons le lecteur aux règlements applicables et à la documentation technique.

La version de FTS disponible au moment de la publication de la présente convention d'utilisation (version 1.0 du document) prend en charge l'eID et la carte d'étranger comme moyen de signature. Son utilisation requiert la saisie du code PIN pour chaque signature apposée par l’utilisateur final. Il est possible de lire les attributs de la carte pendant le processus de signature.

FTS est utilisable sur la dernière et l’avant-dernière version de Windows, macOS ou Linux, en combinaison avec Firefox, Chrome (ou Microsoft Edge) ou Safari. Le fonctionnement de FTS sur d'autres navigateurs et versions est possible, mais aucune garantie ne peut être donnée à cet égard. FTS n’est pas encore disponible sur un appareil mobile.

*eSeal*

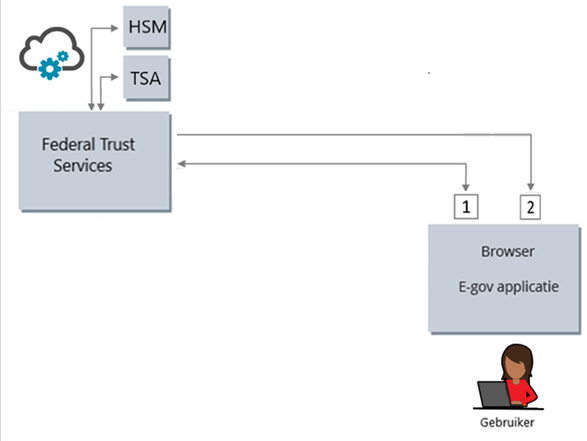
**

FTS permet d’apposer des cachets électroniques avancés ou qualifiés. La version de FTS disponible au moment de la publication de la présente convention d'utilisation (version1.0 du document) peut être intégrée à des produits de fournisseurs externes, mais elle ne dispose pas encore d’une propre infrastructure pour les cachets.

FTS se charge du processus global pour l’apposition du cachet et de l'intégration du cachet dans les données ou dans le document en particulier. La création du cachet par le dispositif nécessite une authentification, et doit donc être effectuée directement par l'utilisateur. Pour solliciter un dispositif de création de cachet, FTS fournit un exemple d’implémentation. Par ailleurs, le service prévoit un support lors de la mise en place d’un processus intégral de création de cachet.

L’apposition de cachet est fortement soumise aux fluctuations de volumes et aux périodes de pointe : c’est la raison pour laquelle des accords contraignants sont conclus avec l’utilisateur dans le document d’onboarding.

*Horodatage*



FTS permet de placer un horodatage qui ancre numériquement de manière irréfutable l'existence d'un ensemble de données ou d'un document (et de son contenu) à une date et une heure données. Personne - y compris le propriétaire des données ou du document - ne peut les modifier sans rompre l’horodatage.

FTS dispose d’un service d’horodatage qualifié. Étant donné que la demande d’un horodatage ne requiert pas d’authentification et que l’horodatage ne comporte pas de données de l’utilisateur, ce processus peut être exécuté de façon autonome par FTS. Il est également possible de proposer de simples *hashes* (empreintes numériques) au service d’horodatage.

L’apposition d’un horodatage est fortement soumise aux fluctuations de volumes et aux périodes de pointe : c’est la raison pour laquelle des accords contraignants sont conclus avec l’utilisateur dans le document d’onboarding.

**Environnements**

La DG TD du SPF BOSA utilise un modèle de développement ouvert où le dernier code source de FTS et toute la documentation technique pertinente sont toujours mis à la disposition du public.

Dès la publication de cette convention d’utilisation, (version du document1.0), la DG TD du SPF BOSA prévoira quatre environnements opérationnels auxquels l’utilisateur pourra avoir accès :

1. L’environnement de production (PRO­D) : la version active de FTS pour les utilisateurs dans le cadre de cette convention ;
2. L’environnement d’intégration (INT) : une copie de production exacte à des fins de test et d’intégration ;
3. L’environnement d’assurance qualité (QA) : pour la validation de nouvelles fonctions ;
4. L’environnement de test et d’acceptation (TA) : pour le test de nouveaux développements.

Les niveaux de service que la DG TD du SPF BOSA propose s’appliquent uniquement à l’environnement de production.

Le code source comprend une démo opérationnelle / implémentation de référence qui montre comment le service peut être intégré dans l’application web de l’utilisateur. Cette démo est mise à disposition en ligne à des fins de démonstration sur tous les environnements, à l’exception de l’environnement de production.

Par ailleurs, il est possible de déployer l'ensemble du service, y compris tous les services web, sur la propre infrastructure de l’utilisateur à des fins de test. La DG TD du SPF BOSA ne fournit un support que pour les environnements FTS qui ont été déployés et sont gérés par la DG TD du SPF BOSA.

Pour plus de détails, nous renvoyons le lecteur à la documentation technique.

## 1.2.Utilisation du service

### 1.2.1. Conditions d’utilisation du service

L’utilisateur prend les mesures organisationnelles et techniques nécessaires pour veiller à ce que FTS soit utilisé et intégré conformément à la présente convention d’utilisation, aux directives de la DG TD du SPF BOSA et à la législation applicable.

L’environnement de production de FTS ne peut être utilisé pour des activités de test de quelque nature que ce soit sans l'accord exprès et écrit de la DG TD du SPF BOSA. Pour les autres environnements, les activités qui pourraient avoir un impact sur les autres utilisateurs (par exemple les stress tests, les tests de charge, etc.) ne peuvent avoir lieu qu'avec l'autorisation explicite de la DG TD du SPF BOSA.

### 1.2.2. Rôles et responsabilités liés à l’utilisateur

L’utilisateur est responsable des aspects suivants :

* le contenu et la qualité des documents proposés et des données liées ;
* l’authentification et l’autorisation correctes de l’utilisateur final ;
* le contrôle du cycle de vie des documents et le respect des accords pour la période de conservation des données ou des documents à signer (upload) et signés (download), tels que repris dans le document d'onboarding ;
* l’intégration correcte et sécurisée de FTS dans le trajet en ligne de l’utilisateur (voir documentation technique de la DG TD du SPF BOSA) ;
* l’interprétation et la traduction correctes des codes et des réponses de FTS (voir documentation technique de la DG TD du SPF BOSA) ;
* le respect des accords en termes de capacité, tels que repris dans le document d’onboarding ;
* la tenue à jour des coordonnées des personnes de contact techniques, via le document d’onboarding.

Si l'utilisateur fait appel à un sous-traitant, il est entièrement responsable du respect par le sous-traitant des obligations de l'utilisateur dans le cadre de la présente convention.

Par l'intermédiaire de son sous-traitant, la DG TD du SPF BOSA offre un service fiable et conforme aux normes et à la législation européennes. Dans le cadre de l'offre du service, une attention particulière est accordée à la sécurité du système et à la protection des données à caractère personnel. La DG TD du SPF BOSA est responsable de la mise à disposition technique du service par l’intermédiaire de son sous-traitant, conformément à la présente convention. Les détails techniques du cahier spécial des charges peuvent être fournis sur demande.

### 1.2.3. Traitement de données à caractère personnel

**Obligations relatives aux données à caractère personnel**

Les Parties s’engagent à respecter le 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 »), ainsi que ses arrêtés d’exécution.

L’utilisateur intervient pour ces traitements en tant que responsable du traitement au sens de l’art. 4, 7° du RGPD :

* via FTS, faire signer les données ou les documents par l’utilisateur final ;
* via FTS, faire apposer un cachet sur les données ou les documents par l’utilisateur ;
* via FTS, faire apposer un horodatage sur les données ou les documents par la DG TD du SPF BOSA.

Le responsable du traitement fournit au sous-traitant les données à caractère personnel liées aux données ou aux documents à signer, à cacheter ou à horodater en vue de ces traitements. Il s'agit des données ou des documents mêmes et, en cas de signature par des tiers, des données des personnes qui doivent être invitées à signer.

Pour ces traitements, la DG TD du SPF BOSA est un sous-traitant du responsable du traitement au sens de l’art. 4, 8° du RGPD. À la demande de l’utilisateur, la DG TD du SPF BOSA exécute la transaction demandée via FTS.

Les données seront conservées par le sous-traitant pendant une période maximum de 5 jours à partir du moment où l'utilisateur a téléchargé les données ou les documents. Ensuite, le document et les données fournies par l’utilisateur sont détruits. L’utilisateur détermine le délai de conservation par la DG TD du SPF BOSA, avec un maximum de 5 jours.

Le sous-traitant traitera les données conformément aux instructions du responsable du traitement.

Sauf si le responsable du traitement lui en donne expressément l’autorisation ou l’instruction, le sous-traitant s’engage à ne communiquer les données qu’à son sous-traitant : SOPRA STERIA, avenue Arnaud Fraiteur 15-23, 1050 Ixelles.

Le sous-traitant tient un registre des activités de traitement qu'il réalise pour le responsable du traitement. Le RGPD, et plus précisément l’« *article 30 - Registre des activités de traitement* », énumère les éléments qui doivent être repris dans le registre. Sur simple demande raisonnable du responsable du traitement, le sous-traitant est tenu de présenter ce registre.

Le sous-traitant s’engage 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.

À tout moment, le responsable du traitement peut demander au sous-traitant une copie des données qui sont traitées dans le cadre du présent marché au format convenu entre les parties.

Par ailleurs, le sous-traitant ne peut pas copier les données mises à disposition, sauf à des fins de sauvegarde, ou si la copie est nécessaire pour exécuter le marché décrit dans le présent contrat. Les mêmes restrictions et obligations que celles applicables aux données originales s’appliquent aux éventuelles copies de données.

À la demande du responsable du traitement, le sous-traitant mettra immédiatement à disposition et/ou détruira irrémédiablement toutes les copies des données traitées, provenant du responsable du traitement ou traitées pour le compte du responsable du traitement.

Le sous-traitant n’enregistrera jamais les données dans un lieu situé en dehors de l’Espace économique européen et ne les transmettra jamais à des pays situés en dehors de l’Espace économique européen. Par ailleurs, le sous-traitant n’enregistrera pas les données à un endroit situé en dehors du territoire belge, sans l’autorisation écrite préalable du responsable du traitement. Le responsable du traitement peut assortir son autorisation de conditions.

Le sous-traitant documente toutes les mesures qu'il prend afin de protéger les données, et le responsable du traitement peut à tout moment demander au sous-traitant de justifier les mesures de protection prises et de fournir les informations nécessaires en la matière.

Le sous-traitant désigne un délégué à la protection des données et dispose au moins d’une politique et d'un plan de sécurité actuels qui seront révisés annuellement.

Le sous-traitant aidera le responsable du traitement à s'acquitter de l’obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits et à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD.

Si les parties prennent connaissance d'une violation des données à caractère personnel mises à disposition, elles s’en informent mutuellement dans les meilleurs délais.

Pour les données figurant dans sa partie de la piste d'audit, la DG TD du SPF BOSA est le responsable du traitement. La piste d’audit comporte les données suivantes : l'identité de l'utilisateur, le numéro d'identification des données ou du document, l'heure du chargement, du téléchargement, de la suppression des données ou du document, l'heure de la signature, du cachet, l'horodatage, le numéro d'identification du signataire. L’utilisateur est responsable du traitement pour sa partie de la piste d’audit. Les deux parties prendront les mesures nécessaires pour sauvegarder les données dans une piste d’audit telle que définie en 1.3.2.

**Mesures techniques et organisationnelles minimales**

Le sous-traitant prendra les mesures techniques et organisationnelles nécessaires et adéquates pour protéger les données contre toute destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de données à caractère personnel.

Le sous-traitant garantit – dans la mesure de ce qui est techniquement possible – l’intégrité, la disponibilité et la confidentialité des données qu’il traite dans le cadre du présent contrat.

Pour ce faire, il doit au minimum mettre en œuvre et utiliser des technologies et des techniques de sécurisation conformes aux meilleures pratiques de l’industrie. Cela implique également des mécanismes visant à détecter et/ou identifier des vulnérabilités et à apporter à temps des correctifs et/ou procéder à temps à des mises à jour.

Les activités des utilisateurs avec les données sont consignées dans des fichiers de journalisation. Il en va de même pour d’autres événements pertinents, tels que des tentatives d’accès non autorisé à des données et des perturbations susceptibles de mener à la modification ou à la perte de données pertinentes.

Le sous-traitant utilise des procédures déterminées pour garantir la disponibilité des informations, des logiciels et d’autres ressources, en ce compris les procédures garantissant la disponibilité pendant les moments critiques.

À tout moment, le responsable du traitement peut communiquer au sous-traitant des informations relatives à des normes de sécurité nouvelles et demander de discuter de l’opportunité d’une adaptation de la méthode de travail du sous-traitant en la matière.

**Accès aux données**

Le sous-traitant veille à ce que les personnes qui travaillent en son nom et pour son compte aient uniquement accès aux données qui sont nécessaires pour accomplir leur tâche ou leur mission dans le cadre du présent contrat. Cela s’applique au personnel permanent ou temporaire et à d’éventuelles parties tierces impliquées directement ou indirectement dans l’exécution du marché.

Au moyen d'une séparation des fonctions, le sous-traitant empêche qu’une combinaison de droits d’accès puisse mener à des actes non autorisés et/ou à un accès non autorisé à des données.

Le sous-traitant prend des mesures afin de prévenir et de détecter des fraudes et toute autre utilisation inappropriée des systèmes et réseaux ou tout accès inapproprié à ces derniers.

Le réseau et les systèmes d’information sont activement surveillés et gérés par le sous-traitant.

Le sous-traitant prévoit les mécanismes d’accès physique et/ou électronique aux systèmes et données du responsable du traitement. Ces mécanismes doivent prévoir une méthode manifestement sécurisée afin d’octroyer un accès aux données.

Le sous-traitant prévoit une liste actualisée du personnel permanent ou temporaire et des éventuelles parties tierces directement ou indirectement impliquées dans l’exécution du marché ainsi que des autorisations dont ils disposent concernant les données à caractère personnel traitées.

Le sous-traitant est responsable de la sécurité et de l’utilisation adéquate des codes d’accès, noms d’utilisateurs et mots de passe (y compris du changement régulier de ces codes et mots de passe) permettant d’accéder aux données à caractère personnel et de les traiter. Le sous-traitant s’engage à tout mettre en œuvre pour que toute personne ayant accès aux données à caractère personnel garde la confidentialité de ses codes d’accès et mots de passe.

**Signaler des incidents**

Le sous-traitant s'engage à notifier au responsable du traitement l’ensemble des (tentatives de) traitements de données ou accès à des données illégitimes ou non autorisés. Le sous-traitant signalera immédiatement à l’adresse suivante tout incident de ce type au responsable du traitement et au plus tard 24h après avoir constaté l’incident : Cliquez ou appuyez pour entrer du texte. Par ailleurs, le sous-traitant prendra toutes les mesures raisonnablement nécessaires pour prévenir ou limiter la violation (ultérieure) des mesures de sécurité.

Dans cette notification, le sous-traitant communiquera au moins les éléments suivants :

* la nature de l’incident
* la date et l’heure de la constatation
* les données impactées
* les mesures directement prises pour limiter les dommages collatéraux
* la date et l’heure de la clôture de l’incident
* les mesures structurelles prises afin d’éviter ce type d'incident à l’avenir.

Le responsable du traitement signalera dans les temps impartis légalement au contrôleur concerné les fuites de données relevant d'une obligation légale de notification.

**Confidentialité**

Le sous-traitant et toute personne agissant en son nom et pour son compte devront respecter une confidentialité stricte des données traitées dans le cadre du présent contrat.

Une exception à cette règle n’est possible que si une prescription légale ou une injonction judiciaire oblige le sous-traitant à communiquer les données ou si les données sont communiquées sur ordre du responsable du traitement. Toute communication légalement obligatoire des données à des tiers doit au préalable être portée à la connaissance du responsable du traitement avant le traitement.

Chacune des personnes ayant accès aux données devra obligatoirement être tenue par une obligation de confidentialité et signer un document à cet effet.

Cette obligation de confidentialité restera en vigueur après le transfert ou la fin du présent contrat.

## 1.3 Sécurité

### 1.3.1. Sécurisation par l'utilisateur

L’accès à FTS n’est possible qu’avec une connexion sécurisée et ce, tant pour les utilisateurs (SSL) que pour les utilisateurs finaux (HTTPS).

L’utilisateur n’a accès à l’environnement de production de FTS que sur la base du compte utilisateur qui lui a été attribué et de l’adresse IP confirmée de l’utilisateur telle que reprise dans le document d’onboarding.

Il incombe à l’utilisateur d’assurer une sécurisation adéquate de ses propres application, données et documents.

### 1.3.2. Piste d’audit

Les parties reconnaissent que la mise en place d’une piste d'audit (*audit trail*) est nécessaire dans le cadre de FTS.

Cette piste d’auditassure que les transactions effectuées via les services web de FTS puissent être reconstituées afin de respecter l’obligation légale de sécuriser suffisamment les données à caractère personnel traitées via FTS. En outre, les données de la piste d'audit peuvent être importantes dans le contexte de la preuve ex post par les parties prenantes.

Les parties reconnaissent que le principe des « cercles de confiance » (*circles of trust*) sera appliqué. De ce fait, chaque partenaire de la chaîne est tenu à titre individuel de prendre les mesures nécessaires pour conserver des données sélectionnées dans sa piste d'audit, 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.

Les parties reconnaissent que, pour ladite reconstitution, chaque partie dépend des données tenues à jour par l’autre partie.

Toutes les parties veillent à ce que ces données restent disponibles pendant une période de 10 ans et à ce qu'elles puissent être fournies sur demande dans un délai de trois jours ouvrables.

Chaque partie est elle-même responsable des procédures et de l’infrastructure qui lui permettront de répondre à ces exigences de manière sécurisée et dans le respect de la vie privée.

# 2. Niveaux de service

La DG TD du SPF BOSA fournira des efforts raisonnables pour atteindre les objectifs de service ci-dessous. Sauf indication contraire, tous les niveaux de service s’appliquent à l’environnement de production de FTS.

## 2.1. Disponibilité et performance

### 2.1.1. Disponibilité et performance du service

Les services web de FTS sont disponibles 24h/24 et 7j/7 avec un objectif de 99,5 % sur une base mensuelle.

Les services web de FTS visent un temps de réponse de l’UI de 3 secondes pour la signature, le cachet et l’horodatage. Cette performance s’applique dans le cadre de la capacité, telle que convenue dans la documentation d’onboarding.

### 2.1.2. Interruption de service planifiée

En cas d'ajustement ou de modification nécessitant une indisponibilité programmée, les utilisateurs en sont informés au préalable par e-mail, conformément aux dispositions du paragraphe 2.3. Cet e-mail contient la date, l'heure de début et la durée de l'interruption, et est envoyé aux personnes de contact spécifiées dans le document d'onboarding.

### 2.1.3. Indisponibilité non planifiée (incident)

En cas d'indisponibilité non planifiée, l'utilisateur est informé par e-mail dans les meilleurs délais de l'incident et du rétablissement du service. Cet e-mail est envoyé aux personnes de contact spécifiées dans le document d’onboarding.

## 2.2. Support

### 2.2.1. Support pour l’utilisateur final (première ligne)

Il est de la responsabilité de l'utilisateur d’offrir un support suffisant (de première ligne) aux utilisateurs finaux en termes d'équipements et de solidité pour les services qu'il propose personnellement. En aucun cas, sauf disposition contraire, le Service Desk de la DG TD du SPF BOSA ne fournira directement des services aux utilisateurs finaux de l'utilisateur.

L’utilisateur ne publiera ou communiquera d’aucune manière les coordonnées de la DG TD du SPF BOSA sans l’autorisation expresse de la DG TD du SPF BOSA.

### 2.2.2. Support supplémentaire (deuxième ligne)

L'ensemble des incidents et demandes sont d’abord notifiés par l’utilisateur au Service Desk de la DG TD du SPF BOSA (support de deuxième ligne). Le Service Desk les transfère ensuite à la bonne personne ou au bon service au sein de la DG TD du SPF BOSA.

La classification et le suivi des incidents sont les suivants :

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification** | **Description de l’incident** | **Canal de notification** | **Temps de réponse (heures de bureau)** |
| **Priorité 1** | Les services web de FTS sont entièrement indisponibles. *(Toutes les applications rencontrent des problèmes et 100 % d’indisponibilité. Ou une violation de données (*data breach*) qui résulte de la responsabilité de la DG TD du SPF BOSA.)* | Téléphone, e-mail | 3h |
| **Priorité 2** | Les services web de FTS sont partiellement indisponibles. *(Certaines applications rencontrent des problèmes. Les utilisateurs de ces applications ne peuvent plus travailler.)* | Téléphone, e-mail | 5h |
| **Priorité 3** | Les services web de FTS sont légèrement affectés. *(Certaines applications rencontrent des problèmes. Les utilisateurs peuvent encore travailler.)* | E-mail, formulaire de contact | 1j |
| **Priorité 4** | Demande informative | E-mail, formulaire de contact | 7j |

En dehors des heures de bureau, ces rôles peuvent être contactés pour des incidents de niveau P1 et P2 :

1. Service manager
2. Product Owner
3. Domain manager.

Toutes les personnes de contact de la DG TD du SPF BOSA sont reprises dans le document d’onboarding.

### 2.2.3. Escalade des incidents

Pour escalader un incident, il faut prendre contact avec le Service manager ou le Service Desk, via les personnes de contact indiquées dans le document d’onboarding. Lors de l’escalade de l’incident, mentionnez toujours le numéro de référence du Service Desk de la DG TD du SPF BOSA.

### 2.2.4. Délégué à la protection des données

Le délégué à la protection des données (*Data protection officer - DPO*) de la DG TD du SPF BOSA peut être contacté à l’adresse [privacy@bosa.fgov.be](mailto:privacy@bosa.fgov.be) pour toute question relative à la protection des données. Les incidents et les plaintes concernant cette thématique sont suivis à l’adresse [privacyincident@bosa.fgov.be](mailto:privacyincident@bosa.fgov.be).

## 2.3. Gestion des modifications

### 2.3.1. Mises à jour planifiées

La DG TD du SPF BOSA s’efforce de procéder aux modifications tout en assurant la continuité du service. Les nouvelles versions peuvent être déployées par défaut sans interruption.

Le schéma diffère selon l’environnement :

* L’environnement TA suit les développements au jour le jour. Ces derniers sont promus par les développeurs dans l'environnement QA lorsqu'ils ont atteint un premier niveau de maturité. Les développements techniques sont déployés automatiquement dès qu’ils sont disponibles dans les codes sources respectifs.
* Pour les environnements INT et PROD, le travail s’effectue sur la base de versions stables du service. Ces versions sont définies lorsqu'un groupe de fonctionnalités forme un ensemble logique et a été testé de manière approfondie dans son ensemble. Le déploiement d'une nouvelle version sur ces environnements est automatique, mais nécessite une décision et un démarrage manuel du processus.

Pour plus de détails, nous renvoyons le lecteur à la documentation technique.

Les modifications de l'environnement de production qui nécessitent une interruption de service seront annoncées à l'utilisateur (personnes de contact spécifiées dans le document d'onboarding) par la DG TD du SPF BOSA un mois à l'avance.

La DG TD du SPF BOSA met tout en œuvre pour assurer une compatibilité maximale avec les versions précédentes. Si, malgré cela, une modification doit être apportée qui ne permet pas de maintenir la compatibilité avec les versions précédentes, la DG TD du SPF BOSA annoncera cette modification et les mesures palliatives à l'utilisateur six mois à l'avance (personnes de contact spécifiées dans le document d'onboarding).

### 2.3.2. Demandes des utilisateurs

La DG TD du SPF BOSA organise périodiquement un FTS User Board (voir 2.5.1.). Les demandes de modification des utilisateurs sont discutées dans ce Board et évaluées sur la base des critères ci-dessous.

|  |  |
| --- | --- |
| Classification | Impact de la modification |
| P1 | Amélioration pour tous les utilisateurs et évaluation minimale des risques*.* |
| P2 | Amélioration pour certains utilisateurs et évaluation minimale des risques*.* |
| P3 | Amélioration pour tous les utilisateurs et évaluation élevée des risques. |
| P4 | Amélioration pour certains utilisateurs et évaluation élevée des risques. |

## 2.4. Composantes du service

Les niveaux de service s’appliquent aux systèmes et aux fonctionnalités de FTS gérés et utilisés par la DG TD du SPF BOSA.

* Accès et utilisation de l'environnement PROD de FTS sur la base du compte utilisateur et de l'adresse IP, comme indiqué dans le document d’onboarding.
* Accès de l’utilisateur à l’environnement INT, QA et TA de FTS sur la base du compte utilisateur, comme indiqué dans le document d’onboarding.
* Renvoi de l'utilisateur final à l'emplacement correct de l'utilisateur avec le statut correct.
* Stockage confidentiel des données et des documents dans les compartiments attribués à l'utilisateur, conformément à la période de sauvegarde indiquée dans le document d'onboarding.
* Accès et utilisation du service web par l'utilisateur final, après renvoi par l'utilisateur.
* Enregistrement d'audit des interactions entre les utilisateurs et les utilisateurs finaux.
* Les composantes logicielles utilisées pour les systèmes et les fonctionnalités de FTS font partie intégrante du service.

Ne font pas partie des niveaux de service :

* Toutes les informations opérationnelles soutenant les services découlant de la présente convention ne font pas partie de cette dernière.
* Les systèmes et fonctionnalités non gérés et utilisés par la DG TD du SPF BOSA, que l'utilisateur utilise/possède pour offrir ses services à son utilisateur final.
* La configuration et le support de l’application de l’utilisateur qui fait l’objet de l’intégration à FTS (*Relying Party*).
* La disponibilité des services externes tels que l’eID et TSA.
* La disponibilité des plateformes externes, dont le navigateur web et les *extension/add-on* *stores*.
* La configuration et le support du matériel de l'utilisateur final, en ce compris mais sans s'y limiter : le navigateur, le système d'exploitation, l’antivirus,…

La DG TD du SPF BOSA n’est pas responsable de la (non) disponibilité de l’application :

* Si la capacité convenue est dépassée structurellement ou inopinément. La DG TD du SPF BOSA ne peut garantir le service FTS que dans le cadre des accords convenus en matière de capacité et de volume dans le document d’onboarding ;
* Par le comportement du navigateur de l'utilisateur ou de l'utilisateur final lorsqu'il s'adresse au service.

L’utilisateur déclare être conscient du fait que la sécurisation des ordinateurs sur lesquels l’application est implémentée ainsi que la sécurisation des mots de passe sont des éléments importants de la sécurité fonctionnelle du système. Le manque de sécurisation de l’environnement de l’utilisateur ou de l’utilisateur final peut donc avoir une influence sur le fonctionnement du système. La DG TD du SPF BOSA ne peut cependant assumer aucune responsabilité pour ce qui est de la sécurisation de l’environnement de l’utilisateur ou de l’utilisateur final dans la mesure où elle n’a pas le moindre contrôle sur celui-ci.

## 2.5. Information, rapports et évaluation

### 2.5.1. Information

La DG TD du SPF BOSA avertira les utilisateurs du service dans les cas suivants :

* Interruption planifiée (voir « Disponibilité ») et modifications (voir « Gestion des modifications »).
* Incident donnant lieu à une interruption de service (voir « Disponibilité »).
* Nouvelles : nouvelles relatives aux services.
* Modification de la convention d’utilisation : en cas de changement apporté à la convention d'utilisation.

L’information est envoyée aux personnes de contact spécifiées dans le document d’onboarding.

### 2.5.2. Monitoring

Il n’est pas permis à l’utilisateur de surveiller FTS d’une manière susceptible d’influencer la performance de FTS.

### 2.5.3. Rapports

La DG TD du SPF BOSA évaluera les chiffres et les incidents en matière de disponibilité et les partagera lors du FTS User Board.

## 2.6. Gouvernance

### 2.6.1. FTS User Board

La DG TD du SPF BOSA organise périodiquement un FTS User Board avec les points suivants à l’ordre du jour :

* Évaluation de la disponibilité et des incidents.
* Demandes de modification.

### 2.6.2. Service meeting avec l’utilisateur

Si l’utilisateur le souhaite, un service meeting (récurrent) peut être organisé sur simple demande.

Les demandes d’ajustement du service issues du service meeting sont mises à l’ordre du jour du FTS User Board.

# 3. Parties et signature

Le service est proposé à l’utilisateur par le Service public fédéral Stratégie et Appui, DG Transformation digitale, Boulevard Simon Bolivar 30, 1000 Bruxelles.

L'utilisation du service est soumise aux Conditions générales, à la présente convention d'utilisation ainsi qu'aux directives techniques et autres de la DG TD du SPF BOSA concernant le service.

En signant une convention d'utilisation, l'utilisateur se déclare également d'accord avec les Conditions générales des services de la DG TD du SPF BOSA.

Signé en date du : Cliquez ou appuyez pour entrer du texte.

Nom de l’utilisateur : Cliquez ou appuyez pour entrer du texte.

Représentant de l’utilisateur : Cliquez ou appuyez pour entrer du texte.

Organisation : Cliquez ou appuyez pour entrer du texte.

Numéro BCE : Cliquez ou appuyez pour entrer du texte.

Fonction du représentant : Cliquez ou appuyez pour entrer du texte.

Adresse e-mail du représentant : Cliquez ou appuyez pour entrer du texte.

Signature : Cliquez ou appuyez pour entrer du texte.



# Annexes

## Conditions générales des services de la DG TD du SPF BOSA

Les Conditions générales figurent sur le site web de la DG TD du SPF BOSA : <https://dt.bosa.be/fr/conditions_generales_services_dg_transformation_digitale>

## Informations techniques

La documentation technique et d’onboarding figure sur <https://dtservices.bosa.be/fr> ou est disponible sur demande.

1. La signature électronique qualifiée peut, sous certaines conditions, être assimilée à une signature manuscrite. Il convient cependant de vérifier qu’aucune réglementation spécifique ne prévoie de prescriptions de forme ou de conditions supplémentaires concernant la validité de documents spécifiques. [↑](#footnote-ref-2)