

Principes relatifs au traitement des données à caractère personnel (Politique de confidentialité)

Version 8.0

Applicable à compter du : 09.03.2026

Historique des versions		
Date	Version	Changements
9 mars 2026	8.0	• Informations mises à jour concernant l'étendue des services • Ajout d'informations concernant la politique de confidentialité distincte applicable au service Authentigate • Inclusion des informations concernant les services pour lesquels SK agit en tant que sous-traitant de données • Mise à jour des prestataires d'authentification secondaire des abonnés en tant que source de données à caractère personnel • Mise à jour de la liste des données à caractère personnel traitées • Ajout d'informations sur la possibilité de déposer une plainte auprès de l'autorité belge de la protection des données • Ajout d'une base juridique pour la divulgation de données à caractère personnel fondée sur l'intérêt légitime à des fins de prévention, de détection et d'enquête en matière de fraude, d'utilisation abusive des services ou d'autres incidents de sécurité
10 octobre 2022	7.0	• Mise à jour et réorganisation de la liste des données à caractère personnel traitées • Ajout de l'intérêt légitime comme base juridique pour le traitement et la communication des données à caractère personnel • Ajout des prestataires d'authentification secondaire des abonnés en tant que source de données à caractère personnel • Ajout d'informations sur les cookies • Explications et formulation améliorées
28 septembre 2020	6.0	• Ajout d'informations concernant le portail MyID • Ajout d'informations concernant la zone géographique dans laquelle les données sont traitées • Ajout d'informations sur la possibilité de déposer une plainte auprès des autorités de contrôle lettones et lituaniennes • Mise à jour de la structure du document • Mise à jour des adresses de sites web et des adresses e-mail
5 décembre 2019	5.0	• Modification de la liste des données à caractère personnel traitées

		• Mise à jour de la structure et du contenu du document • Ajout d'informations concernant le traitement des données à caractère personnel des mineurs • Ajout d'informations concernant le traitement des catégories particulières de données à caractère personnel • Ajout d'informations sur les décisions automatisées • Ajout d'informations sur les sources des données à caractère personnel • Mise à jour des informations relatives à la durée de conservation des données à caractère personnel • Ajout des coordonnées du délégué à la protection des données
10 décembre 2018	4.0	• Modification de la liste des données à caractère personnel traitées • Ajout d'explications concernant les bases juridiques du traitement • Ajout d'informations concernant le transfert de données à caractère personnel vers les services en ligne
25 mai 2018	3.0	Mise à jour conformément aux exigences du Règlement général sur la protection des données (ci-après dénommé « RGPD »), entré en vigueur le 25 mai 2018
1er mars 2018	2.0	• Modification du titre du document • Contenu et structure révisés • Mise à jour de la liste des données à caractère personnel collectées • Conditions révisées pour la modification des principes • Ajout des informations relatives à la version du document
22 décembre 2011	1.0	Première version publique (Principes relatifs à la protection des données des clients)

1. Informations générales

Ces principes relatifs au traitement des données à caractère personnel décrivent la manière dont SK ID Solutions AS (ci-après dénommée « SK »), en tant que responsable du traitement, garantit la protection des données à caractère personnel conformément à la législation en vigueur tout en proposant Smart-ID et Mobile-ID. Ces principes s'appliquent également à la gestion du cycle de vie des certificats relatifs à la carte d'identité estonienne, à la carte d'identité numérique (digi-ID), à la carte d'identité numérique des résidents électroniques, à la carte de séjour et à la carte d'identité diplomatique délivrées jusqu'au 14 novembre 2025 (inclus). Ces principes ont pour objectif de fournir aux abonnés des informations sur les questions pertinentes liées au traitement des données à caractère personnel et de présenter les principes que SK applique lors du traitement de ces données.

Veuillez noter que le traitement des données à caractère personnel dans le cadre du service Authentigate est décrit dans une politique de confidentialité distincte, disponible sur le site web de SK : <https://www.skidsolutions.eu/resources/data-protection/>.

Dans certains cas, SK peut agir en tant que sous-traitant plutôt qu'en tant que responsable du traitement. Par exemple, lorsque l'authentification via Smart-ID est utilisée dans le cadre du FAS (Service fédéral d'authentification) belge, SK traite des données à caractère personnel pour le compte et sur instruction écrite du responsable du traitement, à savoir le Service public fédéral Stratégie et Appui (SPF BOSA), Direction générale Simplification et Digitalisation (DG SD). Dans ce contexte, SK traite, en tant que sous-traitant, le numéro d'identification unique belge échangé lors de l'authentification ainsi que la piste d'audit sécurisée. Pour plus d'informations, veuillez consulter leur politique de confidentialité.

De même, dans le cadre de la fourniture du service Allkirjoitus.fi, SK agit en tant que sous-traitant et traite les données à caractère personnel pour le compte du responsable du traitement et conformément aux instructions documentées de ce dernier, tandis que l'abonné agit en tant que responsable du traitement conformément aux Conditions générales de SK et aux Conditions d'utilisation du service Allkirjoitus.fi, disponibles sur le site web de SK : <https://www.skidsolutions.eu/resources/general-terms-of-subscriber-agreement/>. Pour plus d'informations, veuillez consulter la politique de confidentialité de l'abonné.

Ces principes ne s'appliquent pas au stockage et au traitement des données relatives aux personnes morales ou à d'autres institutions.

Si vous avez des questions concernant le traitement des données à caractère personnel, nous vous invitons à nous contacter aux coordonnées suivantes :

Responsable du traitement :

SK ID solutions AS

Adresse : Pärnu mnt 141, 11314 Tallinn, Estonie

Téléphone : +372 610 1880

E-mail: [info\[A\]skidsolutions.eu](mailto:info[A]skidsolutions.eu)

Fax : +372 610 1881

Numéro d'immatriculation : 10747013

Délégué à la protection des données :

E-mail : [dpo\[A\]skidsolutions.eu](mailto:dpo[A]skidsolutions.eu)

2. Définitions

Nous expliquons ensuite les définitions et les abréviations utilisées dans les présents principes.

2.1. Qu'est-ce que le RGPD ?

C'est le 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 qui abroge la directive 95/46/CE.

SK traite les données à caractère personnel conformément au RGPD et aux autres législations applicables en matière de protection des données ; toutefois, veuillez noter qu'en tant que prestataire de services de confiance, SK est également soumis aux exigences spécifiques relatives au traitement des données à caractère personnel prévues par le règlement eIDAS.

2.2. Qu'est-ce que le règlement eIDAS ?

C'est le règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 concernant l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et qui abroge la directive 1999/93/CE.

En tant que prestataire de services de confiance, SK exerce ses activités et fournit ses services conformément au règlement eIDAS. Ce règlement est directement applicable dans l'Union européenne ; il définit les exigences et les conditions relatives à la prestation de différents services de confiance, y compris des exigences spécifiques concernant le traitement des données à caractère personnel.

2.3. Qu'entend-on par « données à caractère personnel » et « traitement des données à caractère personnel » ?

Les données à caractère personnel sont toutes les données concernant une personne physique identifiée ou identifiable, quelle que soit la forme ou le format sous lequel ces données se présentent. Le traitement des données à caractère personnel désigne toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel (notamment la collecte, l'enregistrement, la conservation, la modification, la mise à disposition, la consultation et la communication, etc.), quelle que soit la manière dont ces opérations sont effectuées ou les moyens utilisés.

2.4. Qu'est-ce qu'une tierce personne ?

Une tierce personne (ou un tiers) désigne toute personne (qu'il s'agisse d'une personne morale ou physique) qui n'est ni un client contractuel, ni un employé, ni un sous-traitant agréé de SK.

2.5. Qu'est-ce qu'un responsable du traitement des données ?

Le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui détermine les finalités et les moyens du traitement des données à caractère personnel. Dans le cadre du présent document, SK est le responsable du traitement des données.

2.6. Qu'est-ce qu'un sous-traitant ?

Un sous-traitant est une personne physique ou morale, une autorité publique, un organisme ou toute autre entité qui a été désignée par contrat par SK pour traiter des données à caractère personnel pour le compte du responsable du traitement. Dans certains cas, SK peut agir en tant que sous-traitant plutôt qu'en tant que responsable du traitement. Des exemples de situations dans lesquelles SK agit en tant que sous-traitant sont décrits dans la section « Informations générales » (voir chap. 1).

2.7. Qu'est-ce qu'un certificat ?

Un certificat est un ensemble de données numériques qui permet la signature électronique et la vérification d'identité, et dans lequel la clé publique est associée à la personne physique titulaire du certificat. Les certificats permettant soit la vérification électronique de l'identité, soit la signature électronique, concernent des données à caractère personnel.

2.8. Qu'est-ce qu'un service en ligne ?

Un service en ligne est un système d'information, une application ou un environnement numérique qui utilise les services fournis par SK (Mobile-ID, Smart-ID, carte d'identité) pour l'authentification des personnes ou pour permettre la signature électronique.

2.9. Qu'est-ce qu'une autorité d'enregistrement ?

Une autorité d'enregistrement est une organisation chargée de l'identification et de l'authentification des personnes. En outre, une autorité d'enregistrement peut accepter des demandes de certificat, les vérifier et/ou les transmettre à SK.

3. Les principes de SK en matière de traitement des données à caractère personnel

Nous accordons une grande importance à la confidentialité et à la protection des données à caractère personnel ; c'est pourquoi nous avons mis en place les mesures de sécurité organisationnelles, physiques et informatiques nécessaires pour garantir l'intégrité, la disponibilité et la confidentialité des données.

Nous avons recensé les données à caractère personnel dont nous avons besoin pour fournir nos services et avons précisé la finalité, l'étendue et la durée de conservation de ces données. Nous avons défini des exigences et des instructions à l'intention des employés de SK et des sous-traitants agréés, afin de garantir un traitement correct des données à caractère personnel. Nous n'accordons l'accès aux données à caractère personnel qu'aux employés formés et aux sous-traitants agréés, qui ont fait l'objet d'une vérification des antécédents appropriée. Les employés et le personnel habilité de SK savent qu'ils ne sont autorisés à traiter des données à caractère personnel que dans la mesure où cela est nécessaire à l'exercice de leurs fonctions ou, dans le cas des sous-traitants habilités, au respect de leurs obligations contractuelles.

Nous confirmons que le traitement des données à caractère personnel est licite, loyal, adapté à l'usage prévu, limité au strict nécessaire, sécurisé et transparent. Toutes nos activités sont régies par la législation, les politiques et les principes applicables de l'Union européenne, de l'Estonie et d'autres instances concernées, ainsi que par les présents principes relatifs au traitement des données à caractère personnel. Les politiques et principes de SK sont disponibles sur le site web de SK : <https://www.skidsolutions.eu/en/repository/>.

SK est certifiée selon la norme ISO/IEC 27001: 2013 « Technologies de l'information. Techniques de sécurité. Systèmes de management de la sécurité de l'information. » Il s'agit d'une norme qui définit les exigences relatives aux processus de gestion du système de sécurité de l'information de l'organisation et aux actifs critiques en matière de sécurité de l'information, y compris les mesures de sécurité techniques, physiques et organisationnelles visant à protéger les données à caractère personnel.

4. Sources des données à caractère personnel

SK recueille des données à caractère personnel auprès des sources suivantes :

- Auprès de la personne concernée ;
- Appareils personnels (dans le cas de Smart-ID) ;
- Registres (par exemple, registres de population) ;
- Prestataires de services en ligne ;
- Autorités d'enregistrement, prestataires de services d'identification en ligne et prestataires de services d'authentification secondaire des abonnés (par exemple, les banques, les opérateurs de téléphonie mobile, l'Office de la police et des gardes-frontières, eIDAS-Node).

5. Légalité du traitement des données à caractère personnel

SK traite les données à caractère personnel uniquement de manière loyale et licite. SK confirme qu'elle traite les données à caractère personnel uniquement à des fins clairement définies et légitimes, et qu'elle limite ce traitement au strict minimum nécessaire pour atteindre ces finalités.

Nous traitons les données à caractère personnel sur la base des fondements juridiques suivants :

- **Exécution du contrat** : Le traitement des données à caractère personnel aux fins de l'exécution d'un contrat signifie que nous avons besoin de ces données pour fournir un service de qualité. Nous avons déterminé quelles données à caractère personnel SK doit collecter pour fournir ses services et nous limitons au strict minimum la quantité de données à caractère personnel traitées.
- **Respect des obligations légales** : Le respect des obligations légales désigne le traitement des données à caractère personnel que SK est tenue d'effectuer en vertu de la loi en tant que prestataire de services. Par exemple, nous traitons des données à caractère personnel en réponse à des demandes fondées sur des motifs juridiques émanant des services chargés de l'application de la loi.
- **Consentement** : Dans certains cas, nous traitons des données à caractère personnel sur la base du consentement de la personne concernée. Nous demandons votre consentement, par exemple, pour le traitement des données biométriques lorsque vous utilisez une méthode d'identification biométrique pour enregistrer votre Smart-ID. En outre, nous traitons, sur la base du consentement, les données à caractère personnel contenues dans les demandes qui nous sont adressées. Dans ce cas, le consentement au traitement des données à caractère personnel est donné par l'envoi de la demande à SK.
- **Intérêt légitime** : Dans certains cas, le traitement des données à caractère personnel repose sur un intérêt légitime. Cela signifie que le traitement est nécessaire à SK ou à un tiers à des fins qui prévalent sur les droits de la personne concernée. Sur la base d'un intérêt légitime, nous traitons par exemple certaines données relatives aux appareils pour des raisons de sécurité.

6. Quelles données à caractère personnel traitons-nous et à quelles fins ?

SK traite des données à caractère personnel aux fins suivantes :

- **Émission et gestion des certificats** : SK délivre des identifiants Smart-ID et Mobile-ID ainsi que des certificats pour les documents d'identité estoniens tels que la carte d'identité, la carte d'identité numérique (digi-ID), la carte d'identité numérique des résidents électroniques, la carte de séjour et la carte d'identité diplomatique. SK se charge également de révoquer les certificats et, dans le cas des documents d'identité, de suspendre et de lever la suspension des certificats.
- **Activation de l'utilisation des certificats** : SK permet l'utilisation de Smart-ID, de Mobile-ID et des documents d'identité estoniens à des fins d'authentification et de signature électronique.
- **Traitement des demandes de données à caractère personnel** : Si dans le cas d'une enquête, ou bien si une personne ou une autre autorité demande des données à caractère personnel à SK, nous traitons les données demandées afin de préparer la réponse. Le demandeur doit disposer d'un fondement juridique pour demander ces données. Ces questions portent sur la délivrance et la gestion des services Smart-ID, Mobile-ID et des certificats liés aux documents d'identité, ainsi que sur l'utilisation de ces certificats à des fins d'authentification et de signature électronique.
- **Traitement des demandes contenant des données à caractère personnel** : Si une personne adresse à SK une demande contenant ses données à caractère personnel, SK traite ces données afin de traiter la demande et d'y répondre.

De plus, nous expliquerons plus en détail, pour chaque activité, quel est l'objectif du traitement, quelle est la base juridique de ce traitement et quelles données à caractère personnel nous traitons.

Finalité du traitement	Base juridique	Quelles sont les données à caractère personnel qui sont ou pourraient être traitées ?
Émission et gestion des certificats		
Prestation de services	Le traitement est nécessaire à l'exécution du contrat ; Les données biométriques sont traitées sur la base du consentement	• Prénom(s) et nom(s) de famille de la personne ; • Numéro d'identification personnel et pays ayant délivré ce numéro ; • Coordonnées ; • Langue de communication ; • Données du document d'identité et/ou copie du document d'identité utilisé pour demander les certificats ; • Un formulaire de demande permettant de demander un certificat signé électroniquement ou à la main ; • Posséder le statut de résident estonien ou le statut de résident électronique ; • Mode d'inscription (en ligne ou en agence) et/ou coordonnées de l'agence ; • Données relatives à l'appareil (uniquement en cas d'inscription électronique via Smart-ID et Mobile-ID) ; • Données relatives aux certificats ; • Données relatives au cycle de vie des certificats et aux opérations effectuées par l'utilisateur lors de l'utilisation du service (suspension de certificats, levée de suspension, révocation de certificats, émission d'enveloppes contenant des codes PIN, renouvellement de certificats, vérification des informations relatives à la validité des certificats) ;

		- Données de la carte SIM et opérateur mobile (uniquement dans le cas de Mobile-ID) ; - Date de naissance et numéro de compte Smart-ID (uniquement en cas d'utilisation de Smart-ID) ; - Informations complémentaires pour les demandes de certificat Smart-ID utilisant la méthode d'identification biométrique : pays de résidence de la personne, données supplémentaires issues du document utilisé lors de l'enregistrement (type de document, pays de délivrance, numéro du document, nationalité, date de naissance, sexe, date d'expiration du document, image faciale de la personne, données techniques nécessaires à la vérification de l'authenticité du document), enregistrement vidéo de l'identification biométrique, nombre de tentatives d'enregistrement infructueuses, informations sur la validité du document issues du registre PRADO. - Dans le cas de Mobile-ID et de Smart-ID, nous vérifions, à l'aide du registre de la population, l'exactitude du nom, du numéro d'identification personnel et du statut du demandeur (vivant, décédé) ainsi que, pour les mineurs, les informations relatives aux tuteurs légaux.
Utilisation des certificats à des fins d'authentification ou de signature électronique		
Prestation de services	Le traitement est nécessaire à l'exécution du contrat	- Prénom(s) et nom(s) de famille de la personne ; - Numéro d'identification personnel ; pour les ressortissants non baltiques et non belges, numéro de passeport ou de carte d'identité ; - Adresse IP du système d'information dans lequel les informations relatives à la validité du certificat ont été consultées ; - Numéro de téléphone et langue de communication ; - Adresse IP du réseau utilisée par l'appareil, données de l'appareil, état des codes PIN dans le cas de Smart-ID ; - Prestataire de services en ligne dont les services sont utilisés ; - Lorsque vous utilisez Smart-ID et Mobile-ID, le texte envoyé par le service en ligne vers votre appareil (les données sont hachées). Veuillez noter que lorsque l'authentification Smart-ID est utilisée dans le cadre du FAS (Service fédéral d'authentification) belge, SK traite, en tant que sous-traitant, le numéro d'identification personnel belge échangé lors de l'authentification ainsi que les données associées relatives à la piste d'audit sécurisée.
Demandes de renseignements concernant des données à caractère personnel		

Réponse aux demandes	Selon la demande, la base juridique peut être le consentement, la loi ou l'intérêt légitime Il convient de noter que le demandeur peut être la personne concernée elle-même, ou bien un service d'enquête ou toute autre autorité disposant d'une base juridique pour demander ces données.	Les données demandées par le demandeur.
Demandes contenant des données à caractère personnel		
Réponse aux demandes	Consentement	Données transmises à SK dans la demande.

Lors de l'authentification sur le service en ligne ou de la signature d'un document, des données à caractère personnel (par exemple, le nom et le numéro d'identification personnel) sont transmises au prestataire du service en ligne afin qu'il puisse fournir le service. Cela ne se fait qu'après la saisie du code PIN. La saisie du code PIN vaut consentement à l'envoi des données.

6.1. Traitement des données à caractère personnel des mineurs

Les services SK sont accessibles aux mineurs. Les mineurs doivent obtenir l'accord de leurs parents ou de leur tuteur pour s'inscrire au service Smart-ID, conclure un contrat Mobile-ID et faire une demande de carte d'identité.

Les mineurs peuvent demander une carte Smart-ID Basic sans droits ou à droits limités dans le cadre d'un contrat de services bancaires. Si un parent ou un tuteur légal a donné cette autorisation dans le cadre d'un contrat de services bancaires, le mineur n'aura pas besoin d'une autorisation distincte pour une demande Smart-ID non qualifiée. Pour en savoir plus sur les identifiants Smart-ID certifiés et non certifiés, rendez-vous sur le portail Smart-ID.

Un parent ou tuteur légal assume la responsabilité des conséquences liées à l'utilisation des services fournis par SK (Mobile-ID, Smart-ID, carte d'identité). Ils doivent également expliquer au mineur les conditions d'utilisation des certificats ainsi que les exigences de sécurité liées à l'utilisation du service.

SK traite les mêmes données à caractère personnel pour les mineurs que pour les adultes, ainsi que les informations relatives au consentement des parents ou du tuteur légal et au lien entre l'enfant et ses parents ou son tuteur (voir le tableau au chapitre 6).

6.2. Traitement de catégories particulières de données à caractère personnel

Conformément au RGPD, les catégories particulières de données à caractère personnel peuvent être traitées sur la base du consentement explicite de la personne concernée. Si vous choisissez la méthode

d'identification biométrique pour l'authentification lors de votre inscription à Smart-ID, SK vous demandera votre consentement pour le traitement de vos données personnelles biométriques au cours de la procédure d'inscription. Les données biométriques traitées correspondent à une image faciale extraite d'une vidéo que vous avez enregistrée de vous-même. Le traitement de l'image faciale est nécessaire pour vous identifier lors de la création d'un compte Smart-ID. Par ailleurs, SK peut procéder à des contrôles de suivi sur la base de vos données biométriques afin de garantir la sécurité de votre identité électronique et de vérifier la qualité de la solution technique mise en œuvre.

Les données biométriques ne sont pas traitées dans le cadre d'autres méthodes d'enregistrement Smart-ID, telles que le lien bancaire, l'agence bancaire, Mobile-ID, Smart-ID ou la carte d'identité.

7. Zone géographique concernée par le traitement des données

En règle générale, SK traite vos données à caractère personnel au sein de l'Union européenne ou de l'Espace économique européen. Si nous faisons appel à des sous-traitants agréés situés en dehors de cette zone, nous le faisons sur la base d'une décision d'adéquation adoptée par la Commission européenne (CE), nous signons des clauses contractuelles types avec le partenaire ou nous mettons en place d'autres garanties appropriées.

8. Décisions automatisées

En vertu du RGPD, toute personne a le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé et produisant à son égard des effets juridiques ou des effets tout aussi significatifs. Des décisions automatisées peuvent être prises s'il est nécessaire d'exécuter un contrat entre un responsable du traitement et une personne, si la loi l'autorise ou si la personne a donné son consentement explicite.

SK prend des décisions automatisées sur la base de vos données biométriques (image faciale) à l'aide d'un processeur d'identification si vous utilisez une méthode d'identification biométrique pour créer un compte Smart-ID. Dans ce cas, SK vous demandera votre consentement lors de la procédure d'inscription. Ces décisions automatisées ne s'appliquent pas aux autres méthodes d'enregistrement Smart-ID, telles que le lien bancaire, l'agence bancaire, Mobile-ID, Smart-ID ou la carte d'identité.

SK prend également des décisions automatisées concernant la délivrance ou le refus de délivrance de certificats sur la base des données obtenues auprès des registres et valide les demandes de certificats électroniques par le biais d'une décision automatisée.

De plus, nous prenons des décisions automatisées afin de prévenir et de détecter les activités frauduleuses.

9. Droits de la personne concernée

La personne concernée a le droit d'accéder à ses données à caractère personnel, d'en demander la rectification, l'effacement, la portabilité et la limitation du traitement.

Pour exercer les droits énumérés ci-dessus, vous pouvez envoyer une demande signée électroniquement à l'adresse e-mail [info\[A\]skidsolutions.eu](mailto:info[A]skidsolutions.eu). Nous répondrons à votre demande dans un délai de 30 jours.

Nous tenons à souligner que la demande ne peut être satisfaite dans les cas suivants :

- l'identité du demandeur ne peut être établie ;
- le demandeur n'a aucun lien juridique avec les données ;
- cela serait contraire aux dispositions des lois spéciales ;
- cela serait contraire aux obligations légales de SK ;
- cela pourrait porter atteinte aux droits et libertés d'autrui ;
- cela pourrait entraver la prestation du service ou entraîner une interruption de celui-ci ;
- cela pourrait entraver le travail des forces de l'ordre ;
- ce n'est pas techniquement possible.

De plus, vous pouvez accéder à vos comptes Mobile-ID, Smart-ID, carte d'identité et digi-ID, ainsi qu'à leur historique, sur le portail MyID. Pour la carte d'identité, la carte d'identité numérique digi-ID et Mobile-ID, vous pouvez également consulter l'historique de toutes vos transactions (authentification et signature) à partir de cette page. Vous trouverez des informations concernant vos comptes Smart-ID et les opérations effectuées via Smart-ID sur le portail Smart-ID.

Si le traitement des données à caractère personnel repose sur votre consentement, vous pouvez à tout moment retirer ce consentement en envoyant une demande signée électroniquement à l'adresse e-mail [info\[A\]skidsolutions.eu](mailto:info[A]skidsolutions.eu).

Si vous estimez que vos droits en matière de traitement des données à caractère personnel ont été violés, nous vous invitons à envoyer une réclamation signée électroniquement par e-mail à l'adresse [dpo\[A\]skidsolutions.eu](mailto:dpo[A]skidsolutions.eu). Nous répondrons à votre e-mail dans un délai de 30 jours. Si vous constatez que SK ne traite pas vos données à caractère personnel conformément à la législation applicable, vous pouvez déposer une plainte auprès de l'autorité nationale chargée de la protection des données de votre pays (par exemple, l'Inspection estonienne de la protection des données, l'Inspection lettone de la protection des données, l'Inspection lituanienne de la protection des données ou l'Autorité belge de protection des données).

10. Utilisation des données par un sous-traitant agréé

En vertu du contrat, SK a le droit d'autoriser une autre personne (qu'il s'agisse d'une personne physique ou morale) à traiter des données à caractère personnel. Les prestataires agréés sont, par exemple, les partenaires de SK chargés de la délivrance et de la gestion des certificats, ainsi que du traitement des problèmes rencontrés par les clients. En tant que responsable du traitement, SK fournit au sous-traitant agréé les instructions nécessaires au traitement des données. SK est responsable du respect, par le sous-traitant mandaté, des exigences relatives au traitement des données à caractère personnel. Un sous-traitant agréé ne peut traiter des données à caractère personnel que dans le but de réaliser l'objectif visé. SK confirme que des accords relatifs au traitement des données seront conclus avec tous les sous-traitants agréés. La liste des sous-traitants agréés de SK est disponible [ici](#).

Un service en ligne qui demande vos données à caractère personnel à SK sur la base d'une authentification ou d'une signature électronique que vous avez initiée n'est pas le sous-traitant mandaté par SK au sens du RGPD.

11. Divulgarion ou communication de données à caractère personnel à des tiers

SK ne communique ni ne transmet de données à caractère personnel à des tiers, sauf dans les cas suivants :

- Une telle obligation découle de la législation applicable ou des mesures adoptées en vertu de celle-ci (par exemple, la transmission à une autorité chargée des enquêtes) ;
- Ces parties participent à la prestation des services ;
- Le tiers a un intérêt légitime à demander ces données à SK ;
- Aux fins de prévention, de détection et d'enquête en matière de fraude, d'utilisation abusive du service ou d'autres incidents de sécurité, lorsque SK ou une autre partie a un intérêt légitime à ce traitement ;
- SK est en droit, aux fins de l'exécution d'un contrat ou pour garantir cette exécution, de communiquer les données à des tiers, notamment à des agences d'évaluation du crédit et de recouvrement de créances ainsi qu'à d'autres personnes chargées du traitement des créances, ainsi qu'à des conseillers juridiques et à des huissiers de justice si la personne concernée n'a pas respecté le contrat ;
- La personne concernée donne son consentement écrit à la communication de ces informations à d'autres tiers.

SK confirme qu'elle ne communiquera des données à caractère personnel à des tiers que dans la mesure où cela est nécessaire aux fins pour lesquelles ces données sont traitées.

SK communique vos certificats estoniens valides liés aux documents d'identité (y compris les Mobile-ID délivrés jusqu'au 2 juillet 2022) pendant leur période de validité via le service LDAP. Vous trouverez plus d'informations sur le service LDAP [ici](#).

12. Durée de conservation des données à caractère personnel

SK traite les données à caractère personnel uniquement pendant la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées ou au respect des obligations découlant de la législation applicable. Veuillez noter que, dans le cadre de la fourniture de services de confiance, nous nous conformons au règlement eIDAS et à la loi estonienne sur l'identification électronique et les services de confiance pour les transactions électroniques en ce qui concerne le stockage des données à caractère personnel.

SK est tenue de conserver les éléments de preuve utilisés pour vous identifier lors de la délivrance des certificats pendant au moins dix ans après l'expiration de ceux-ci, ainsi que les journaux relatifs aux procédures effectuées dans le cadre de la fourniture de services de confiance pendant au moins dix ans, afin de pouvoir, si nécessaire, prouver toute utilisation abusive de votre identité et le caractère approprié des opérations menées par SK dans le cadre de la fourniture de ses services. La conservation des données et des preuves est exigée par la loi et vérifiée par des auditeurs indépendants et des organismes de contrôle.

13. Cookies

SK utilise des cookies sur ses sites web. Les cookies sont utilisés conformément aux politiques en matière de cookies des sites web, disponibles sur [le site web de SK](#).

14. Modification des principes régissant le traitement des données à caractère personnel

SK se réserve le droit de modifier unilatéralement ces principes relatifs au traitement des données à caractère personnel, conformément aux exigences prévues par la législation applicable. Les modifications seront publiées sur [le site web de SK](#) et entreront immédiatement en vigueur.

