

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

Version 7.0

En vigueur à partir du : 10.10.2022

Version et changements		
Date	Version	Changements
10 octobre 2022	7.0	<ul style="list-style-type: none"><li>• Mise à jour et réorganisation de la liste des données à caractère personnel traitées</li><li>• Ajout de l'intérêt légitime comme base légale du traitement et de la divulgation des données à caractère personnel</li><li>• Ajout des fournisseurs d'authentification secondaires comme source de données à caractère personnel</li><li>• Ajout d'informations relatives aux cookies</li><li>• Explications et formulations améliorées</li></ul>
28 septembre 2020	6.0	<ul style="list-style-type: none"><li>• Ajout d'informations à l'égard du MyID portal</li><li>• Ajout d'informations relatives à la zone géographique du traitement des données</li><li>• Ajout d'informations sur la possibilité d'introduire une réclamation auprès des autorités de contrôle Lithuaniennes et Lettones</li><li>• Mise à jour de la structure du Document</li><li>• Mise à jour des adresses du site web et des adresses de messagerie électronique</li></ul>
5 décembre 2019	5.0	<ul style="list-style-type: none"><li>• Amendement de la liste des données à caractère personnel traitées</li><li>• Mise à jour de la structure et du contenu du document</li><li>• Ajout d'informations relatives au traitement des données à caractère personnel sur des personnes mineures</li><li>• Ajout d'informations relatives au traitement de catégories particulières de données à caractère personnel</li><li>• Ajout d'informations relatives aux décisions automatisées</li><li>• Ajout d'informations sur les sources de données à caractère personnel</li><li>• Mise à jour des informations relatives à la période de conservation des données à caractère personnel</li><li>• Ajout des coordonnées de contact du délégué à la protection des données</li></ul>

10 décembre 2018	4.0	<ul style="list-style-type: none"><li>• Amendement de la liste des données à caractère personnel traitées</li><li>• Ajout d'explications à l'égard des bases légales du traitement</li><li>• Ajout d'informations relatives à la portabilité des données à caractère personnel vers un service électronique</li></ul>
25 mai 2018	3.0	<ul style="list-style-type: none"><li>• Mise à jour conformément aux exigences du Règlement général sur la protection des données (ci-après « RGPD », entré en vigueur le 25 mai 2018</li></ul>
1 <sup>er</sup> mars 2018	2.0	<ul style="list-style-type: none"><li>• Changement du titre du document</li><li>• Révision du contenu et de la structure</li><li>• Mise à jour de la liste des données à caractère personnel collectées</li><li>• Révision des conditions relatives à l'amendement des principes</li><li>• Ajout d'informations de la version du document</li></ul>
22 décembre 2011	1.0	<ul style="list-style-type: none"><li>• Première version publique (Principes relatifs à la protection des données client)</li></ul>

## 1. Informations générales

Ces principes de traitement des données à caractère personnel décrivent comment SK ID Solutions AS (ci-après "SK") assure, en tant que contrôleur de données, la protection des données à caractère personnel conformément aux lois applicables tout en offrant un service de Smart-ID et de Mobile-ID ainsi qu'un service de certification des cartes d'identité Estoniennes, des identités numériques (digi-ID), des e-résidents digi-ID, de la carte de permis de séjour et de la carte d'identité diplomatique. L'objectif de ces principes est de fournir des informations pertinentes aux abonnés sur les sujets portant sur le traitement des données à caractère personnel et de présenter les principes suivis par SK lors du traitement des données à caractère personnel.

Ces principes ne concernent ni le stockage ni le traitement de données des personnes morales ou d'autres institutions.

Pour toute éventuelle question à propos du traitement des données à caractère personnel, merci de bien vouloir nous contacter par le biais des contacts ci-dessous :

### Contrôleur de données :

#### SK ID Solutions AS

Adresse : Pärnu mnt 141, 11314 Tallinn, Estonie

Téléphone : +372 610 1880

Courriel : [info@skidsolutions.eu](mailto:info@skidsolutions.eu)

Fax : +372 610 1881

**Code d'enregistrement :** 10747013

**Délégué à la protection des données :**

**Courriel :** [dpo\[A\]skidsolutions.eu](mailto:dpo[A]skidsolutions.eu)

## 2. Définitions

Ci-après nous expliquons les définitions et les abréviations utilisées dans les présents principes.

### 2.1. Qu'est-ce que le RGPD ?

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 abrogeant la directive 95/46/EC.

SK assure le traitement des données à caractère personnel conformément au RGPD et d'autres législations pertinentes sur la protection des données, cependant, veuillez noter qu'en tant que prestataire de service de confiance, SK est également guidé par les exigences particulières relatives au traitement des données à caractère personnel stipulées dans le règlement eIDAS.

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

Le règlement (EU) 910/2014 du Parlement Européen et du Conseil du 23 Juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

En tant que prestataire de services de confiance, SK est guidé par le règlement eIDAS en ce qui concerne ses activités et sa prestation de service. Le règlement est applicable directement dans l'Union Européenne, contenant des exigences et des conditions pour la prestation de différents services de confiance, y compris des exigences particulières sur le traitement des données à caractère personnel.

### 2.3. Quelles sont les données à caractère personnel et en quoi consiste le traitement des données à caractère personnel ?

Les données à caractère personnel sont toute information se rapportant à une personne physique identifiable ou susceptible d'être identifiée, indépendamment de la forme ou du format de ces données. Un traitement des données à caractère personnel est une opération, ou tout ensemble d'opérations, appliquée à des données à caractère personnel, (y compris la collecte, l'enregistrement, la conservation, la modification, l'autorisation d'accès, l'extraction et la communication etc.), quel que soit le procédé ou les moyens utilisés pour l'exécution de ces opérations.

### 2.4. Qu'est-ce qu'un tiers ?

Un tiers est toute personne (à la fois physique et morale) qui n'est pas un client contractuel, un employé ou un sous-traitant de données autorisé de SK.

## **2.5. Qu'est-ce qu'un contrôleur de données ?**

Un contrôleur de données est une personne physique ou morale, une autorité publique, un service ou tout autre organisme qui détermine les finalités et les moyens du traitement des données à caractère personnel. Dans le cadre de ce document, SK est le contrôleur de données.

## **2.6. Qu'est-ce qu'un processeur de données ?**

Un processeur de données est une personne physique ou morale, une autorité publique, un service ou tout autre organisme qui a été assigné de manière contractuelle par SK en vue de traiter des données à caractère personnel pour le compte du contrôleur de données.

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

Un certificat est constitué de données numériques qui facilitent la signature électronique et le contrôle d'identité et dans lequel la clé publique est associée à la personne physique titulaire du certificat. Les certificats qui permettent soit un contrôle d'identité électronique soit une signature électronique se rapportent aux données à caractère personnel.

## **2.8. Qu'est-ce qu'un e-service ?**

Un e-service est un système d'information, une application ou un environnement électronique qui utilise les services fournis par SK (cartes d'identité, Mobile-ID, Smart-ID) en vue d'authentifier des personnes ou de permettre une signature électronique.

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

Une autorité d'enregistrement est une entité qui vérifie l'identité et qui authentifie les personnes. De plus, une autorité d'enregistrement peut accepter des demandes de certificats, les vérifier et/ou les envoyer à SK.

## **3. Les principes de SK à l'égard du traitement des données à caractère personnel**

Nous accordons une importance primordiale à la confidentialité et à la protection des données à caractère personnel. Par conséquent, nous avons pris les mesures de sécurité nécessaires physiques, d'organisation et de technologie d'information pour assurer l'intégrité, la disponibilité et la confidentialité des données.

Nous avons cartographié les données à caractère personnel dont nous avons besoin pour la prestation de nos services et spécifié la finalité, la portée et la période nécessaires pour la conservation de ces données. Nous avons établi les exigences et les instructions destinées aux employés et aux processeurs de données autorisés de SK, sur la façon de traiter les données à caractère personnel correctement. Nous n'avons accordé l'accès aux données à caractère personnel qu'aux employés formés et aux

processeurs de données autorisés ayant passé un contrôle des antécédents approprié. Les employés et personnel agréé de SK sont conscients qu'ils ont le droit de traiter les données à caractère personnel uniquement dans la mesure nécessaire à l'exécution de leurs missions, ou, dans le cadre des processeurs de données, pour satisfaire leurs obligations contractuelles.

Nous confirmons que le traitement des données à caractère personnel est légitime, loyal, pertinent, limité au strict nécessaire, sécurisé et transparent. Toutes nos activités sont menées dans le respect de la législation applicable de l'UE, de l'Estonie et de toute autre réglementation pertinente, ainsi que des politiques, principes de SK ainsi que des 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 par la norme ISO/IEC 27001 : 2013 « Technologies de l'information. Techniques de sécurité. Systèmes de gestion de la sécurité. » Il s'agit d'une norme qui spécifie les exigences pour les processus de gestion des systèmes de la sécurité des informations de l'organisation et pour les actifs de sécurité des informations critiques, y compris les mesures de sécurité techniques, physiques et structurelles afin de protéger les données à caractères personnel.

## 4. Sources de données à caractère personnel

SK obtient des données à caractère personnel à partir des sources suivantes :

- de la personne concernée ;
- Appareils personnels (dans le cas d'une Smart-ID) ;
- Registres (par ex. registres de la population) ;
- Prestataires d'E-service ;
- Autorités d'enregistrement, prestataires d'identification électronique et fournisseurs d'authentification secondaires (par ex. banques, opérateurs de téléphonie mobile, les services de police et les gardes-frontières).

## 5. Licéité du traitement des données à caractère personnel

SK ne traite les données à caractère personnel que de manière loyale et licite. SK confirme traiter les données à caractère personnel uniquement pour des finalités légitimes et clairement déterminées et limite le traitement des données à caractère personnel au strict minimum nécessaire pour satisfaire ces finalités.

Nous traitons les données à caractère personnel suivant les bases légales suivantes :

- **Exécution de contrat** : le traitement de données à caractère personnel pour l'exécution d'un contrat signifie que nous avons besoin de données à caractère personnel afin de fournir un service de qualité. Nous avons déterminé les données à caractère personnel dont SK a besoin pour fournir ces services et nous maintenons la quantité des données à caractère personnel traitées au strict minimum.
- **Conformité à des contraintes légales** : la conformité à des contraintes légales se rapporte au traitement des données à caractère personnel que SK doit satisfaire, conformément à la loi, en tant que prestataire de service. Par exemple, nous traitons des données à caractère

personnel en réponse à des requêtes légalement motivées provenant d'autorités chargées 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 un consentement, par exemple, pour le traitement de données biométriques dans le cadre de l'utilisation de procédés d'identification biométrique pour l'enregistrement d'une Smart-ID. De plus, nous traitons sur la base du consentement des données à caractère personnel en réponse à des requêtes contenant des données à caractère personnel. Dans ce cas, le consentement pour le traitement des données à caractère personnel est fourni en envoyant la requête à SK.
- **Intérêt légitime** : dans certains cas, le traitement des données à caractère personnel est fondé sur un intérêt légitime. Cela signifie que le traitement est nécessaire pour SK ou pour une tierce partie pour une finalité qui prévaut aux droits de la personne concernée. Sur la base de l'intérêt légitime, nous traitons par exemple, certaines données d'appareil pour des raisons de sécurité.

## 6. Quelles données à caractère personnel et pour quelles finalités les traitons-nous ?

SK traite des données à caractère personnel pour les finalités suivantes :

- **Emettre et délivrer des certificats** : SK émet des Smart-ID, Mobile-ID et des certificats pour des documents d'identité Estoniens, comme une carte d'identité, une carte d'identité numérique (digi-ID, e-resident), une carte de permis de séjour et une carte d'identité diplomatique. SK se charge également de révoquer les certificats et, dans le cas des documents d'identité, à suspendre et à mettre fin à la suspension des certificats.
- **Permettre l'utilisation des certificats** : SK autorise l'utilisation des Smart-ID, Mobile-ID et des documents d'identité Estoniens à des fins d'authentification et de signature électronique.
- **Gérer des requêtes demandant des données à caractère personnel** : au cas où une personne en fait la demande personnellement ou une enquête ou une autre autorité réclame des données à caractère personnel à SK, nous traitons les données à caractère personnel requises pour rédiger la réponse. Le demandeur doit disposer d'une base légale pour demander les données. Les requêtes concernent l'émission et la délivrance de Smart-ID, Mobile-ID et de certificats de documents d'identité et/ou l'utilisation des certificats à des fins d'authentification et de signature électronique.
- **Gérer des requêtes contenant des données à caractère personnel** : au cas où une personne envoie à SK une requête quelconque contenant ses données à caractère personnel, SK traite les données pour prendre en charge la requête et y répondre.

En outre, nous allons expliquer de manière plus détaillée, pour chaque activité, la finalité du traitement, la base légale du traitement et les données à caractère personnel que nous traitons.

Finalité du traitement	Base légale	Quelles sont les données à caractère personnel qui sont ou sont susceptibles d'être traitées ?
<b>Émettre et délivrer des certificats</b>		
Fourniture de service	Le traitement est nécessaire pour satisfaire le contrat ;	<ul style="list-style-type: none"><li>• Noms et prénoms de la personne ;</li><li>• Numéro d'identification personnel et le pays ayant délivré le code d'identification personnel ;</li></ul>

	<p>Les données biométriques sont traitées sur la base d'un consentement</p>	<ul style="list-style-type: none"><li>• Coordonnées de contact ;</li><li>• Langue de communication ;</li><li>• Données de document d'identité et/ou une copie du document d'identité utilisé pour la demande des certificats ;</li><li>• Un formulaire de demande pour demander que le certificat soit signé électroniquement ou manuellement ;</li><li>• Existence d'un titre de séjour Estonien ou d'un titre e-residency ;</li><li>• Procédé d'enregistrement (électronique ou à un point de service clientèle) et/ ou données du point de service clientèle ;</li><li>• Données d'appareil (uniquement dans le cas d'un enregistrement électronique par Smart-ID et Mobile-ID) ;</li><li>• Données de certificats ;</li><li>• Données relatives au cycle de vie du certificat et aux opérations effectuées par la personne utilisant le service (suspension de certificats, terminaison de suspension, révocation de certificats, émission d'enveloppes à PIN, renouvellement de certificats, vérification d'informations de la validité d'un certificat) ;</li><li>• Données de carte SIM et opérateur de téléphonie mobile (uniquement dans le cas d'une Mobile-ID) ;</li><li>• Date de naissance et numéro de compte Smart-ID (uniquement dans le cas d'une Smart-ID) ;</li><li>• Informations supplémentaires pour des requêtes de certificat de Smart-ID à l'aide du procédé d'identification biométrique ; le pays de résidence de la personne, des données supplémentaires émanant du document utilisé à l'enregistrement (type de document, pays de délivrance, numéro de document, citoyenneté, date de naissance, sexe, date d'expiration du document, image faciale de la personne, données techniques nécessaires pour la vérification de l'authenticité du document), vidéo enregistrée lors de l'identification biométrique, nombre d'échecs de tentatives d'enregistrement, informations sur la validité du document émanant du registre PRADO.</li><li>• Dans le cas d'une Mobile-ID et d'une Smart-ID nous procédons à une vérification auprès du registre de la population, l'exactitude du nom, du numéro d'identification personnel, la situation du demandeur (vivant, décédé) et dans le cas d'une personne mineure, des informations concernant les tuteurs légaux.</li></ul>
--	-----------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<b>Utilisation des certificats pour une authentification ou une signature électronique</b>		
Fourniture de service	Le traitement est nécessaire pour satisfaire le contrat ;	<ul style="list-style-type: none"> <li>Noms et prénoms de la personne ;</li> <li>Numéro d'identification personnel, pour les citoyens en dehors des Baltiques, le passeport ou un numéro de carte d'identité ;</li> <li>Adresse IP du système d'information dans lequel des informations de validité d'un certificat ont été demandées ;</li> <li>Numéro de téléphone et langue de communication ;</li> <li>Adresse IP de réseau utilisé par l'appareil, données d'appareil, état des codes PIN dans le cas d'une Smart-ID;</li> <li>Prestataire d'E-service dont le service est utilisé ;</li> <li>Lors de l'utilisation d'une Smart-ID et d'une Mobile-ID, le texte envoyé à votre appareil par e-service.</li> </ul>
<b>Requêtes réclamant des données à caractère personnel</b>		
Répondre à la requête	<p>En fonction de la requête, la base légale peut être un consentement, la loi ou un intérêt légitime</p> <p>Veillez noter que le demandeur peut être la personne concernée, ou une enquête ou une autre autorité ayant une base légale pour réclamer les données.</p>	Données qui sont demandées par le demandeur/la demanderesse.
<b>Requêtes contenant des données à caractère personnel</b>		
Répondre à la requête	Consentement	Données qui sont transmises à SK dans la requête.

Lors de l'authentification auprès d'un e-service ou la signature d'un document, des données à caractère personnel (par ex. le nom et le numéro d'identification personnel) sont envoyées à un prestataire d'e-service pour fournir le service. Cela n'est réalisé qu'une fois qu'un code PIN est saisi. La saisie d'un code PIN constitue un consentement à l'envoi des données.

## 6.1. Traitement des données à caractère personnel de personnes mineures

Les services SK sont disponibles pour être utilisés par des mineurs. Les personnes mineures doivent avoir le consentement parental ou celui de leur tuteur légal pour l'enregistrement d'une Smart-ID qualifiée, en passant un contrat de Mobile-ID et des demandes de carte d'identité.

Les personnes mineures peuvent demander une Smart-ID Basic non-qualifiée ou aux droits limités, dans le cadre d'un contrat de service bancaire. Si un parent ou un tuteur légal a accordé une telle

autorisation par le biais d'un contrat de service bancaire, une personne mineure n'aura pas besoin d'une autorisation séparée pour une demande de Smart-ID non qualifiée. Vous pouvez en savoir plus sur les Smart-ID qualifiées et non-qualifiées sur le portail de Smart-ID.

Le parent ou tuteur légal endosse la responsabilité liée à l'utilisation des services fournis par SK (Mobile-ID, Smart-ID, carte d'identité). Il doit également expliquer à la personne mineure les clauses et conditions d'utilisation des certificats et les exigences en termes de sécurité de l'utilisation de service.

SK traite les mêmes données à caractère personnel pour les personnes mineures que celles des adultes, ainsi que les informations concernant le consentement parental ou du tuteur légal et le lien entre l'enfant et le parent/ tuteur (voir le tableau au chapitre 6).

## **6.2. Traitement de catégories particulières de données à caractère personnel**

Conformément au RGPD, des catégories particulières de données à caractère personnel peuvent être traitées sur la base du consentement explicite de la personne. Si vous sélectionnez le procédé d'identification biométrique à l'enregistrement d'une Smart-ID, SK demandera votre consentement afin de traiter vos données biométriques personnelles pendant la procédure d'enregistrement. Les données biométriques traitées sont une image de votre visage extraite d'une vidéo que vous avez enregistré de vous-même. Le traitement de l'image faciale est nécessaire pour vous identifier pendant l'enregistrement d'un compte de Smart-ID. De plus, SK peut effectuer des vérifications ultérieures sur la base de vos données biométriques pour assurer la sécurité de votre identité électronique et pour tester la qualité de la solution technique utilisée.

Les données biométriques ne sont pas traitées dans le cas d'autres procédés d'enregistrement de Smart-ID, comme un lien bancaire ou une agence, une Mobile-ID, Smart-ID, carte d'identité.

## **7. Zone géographique du 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. Au cas où nous impliquons des processeurs autorisés situés en dehors de cette zone, nous le faisons sur la base d'une décision adéquate prise par la Commission Européenne (CE), d'une signature de clauses contractuelles standard avec le partenaire ou de la mise en œuvre d'autres protections appropriées.

## **8. Décisions automatisées**

Conformément au RGPD, une personne a le droit qu'aucune décision basée uniquement sur un traitement automatisé ne soit faite les concernant entraînant des conséquences légales ou d'une importance similaire sur eux. Des décisions automatisées pourraient être réalisées si cela est nécessaire pour l'exécution d'un contrat entre un contrôleur et une personne, autorisé par la loi ou à la suite du consentement explicite de la personne.

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 le procédé d'identification biométrique pour l'enregistrement d'un compte Smart-ID. Dans ce cas, SK demandera votre consentement pendant le

processus d'enregistrement. Ces décisions automatisées ne sont pas réalisées dans le cas d'autres procédés d'enregistrement, comme un lien bancaire ou une agence, des Mobile-ID, Smart-ID, carte d'identité.

SK prend également des décisions automatisées en ce qui concerne l'émission ou le refus d'émission d'un certificat sur la base de données obtenues à partir de registres et valide des requêtes de certificat électronique par l'intermédiaire d'une décision automatisée.

De plus, nous prenons des décisions automatisées dans le but de prévenir et détecter toute activité frauduleuse.

## 9. Droits de la personne concernée par les données

La personne concernée a le droit d'accès, de rectification, d'effacement à ses données à caractère personnel, de portabilité de ses données et d'exercer son droit à la limitation du traitement.

Pour exercer les droits susmentionnés, vous pouvez envoyer une requête signée électroniquement à l'adresse [info@skidsolutions.eu](mailto:info@skidsolutions.eu). Nous répondrons à votre requête dans un délai de 30 jours.

Il convient de souligner que la requête ne peut pas être satisfaite dans les cas suivants :

- L'identité du demandeur/demanderesse ne peut pas être identifiée ;
- Le demandeur/demanderesse n'est pas légalement lié(e) aux données ;
- Cela serait contraire aux exigences requises par certaines lois particulières ;
- Cela entre en conflit avec les contraintes légales de SK ;
- Cela pourrait porter atteinte aux droits et aux libertés d'une autre personne ;
- Cela pourrait entraver la prestation du service ou faire échouer la prestation ;
- Cela pourrait entraver le travail des forces policières ;
- Cela n'est pas faisable techniquement.

De plus, vous pouvez accéder à vos comptes Mobile-ID, Smart-ID, cartes d'identité et digi-ID et à leur historique sur le portail MyID portal. Pour les cartes d'identité, digi-ID et Mobile-ID vous pouvez également voir l'historique de toutes vos transactions (authentification et signature) sur ce portail. Les informations concernant vos comptes Smart-ID et les transactions effectuées à l'aide de Smart-ID peuvent être retrouvées sur le portail Smart-ID.

Si le traitement des données à caractère personnel repose sur le consentement, vous pouvez retirer votre consentement à tout moment en déposant une requête électroniquement signée au courriel [info@skidsolutions.eu](mailto:info@skidsolutions.eu).

Si vous constatez que vos droits relatifs au traitement de vos données à caractère personnel ont été violés, nous vous prions de bien vouloir envoyer une plainte signée électroniquement au courriel [dpo@skidsolutions.eu](mailto:dpo@skidsolutions.eu). Nous répondrons à votre courriel dans un délai de 30 jours. Si vous trouvez que SK ne traite pas vos données à caractère personnel conformément à la législation pertinente, vous pouvez déposer une plainte auprès de votre autorité de protection des données nationale (par ex. l'inspection de la protection des données Estonienne, l'inspection des données de l'État Lettone, l'inspection de la protection des données de l'État Lithuanien).

## 10. Utilisation des données par l'intermédiaire d'un processeur de données autorisé

SK a le droit, conformément au contrat, d'autoriser une autre personne (à savoir des personnes à la fois physiques et morales) de traiter des données à caractère personnel. Les processeurs autorisés sont, par exemple, les partenaires de SK, responsables de l'émission et de la délivrance de certificats et de la résolution de problèmes liés au client. SK fournit, en tant que contrôleur de données, les instructions nécessaires pour le traitement des données au processeur autorisé. SK est responsable de la conformité du processeur de données autorisé aux exigences du traitement de données à caractère personnel. Un processeur de données autorisé peut traiter des données à caractère personnel uniquement pour atteindre la finalité. SK confirme que des accords de traitement de données seront conclus avec l'ensemble des processeurs autorisés. Une liste des processeurs de données autorisés de SK est disponible [ici](#).

Un e-service qui demande vos données à caractère personnel à SK sur la base d'une authentification ou d'une signature électronique, initiée par vous, ne constitue pas un processeur autorisé de SK conformément au RGPD.

## 11. Divulgarion ou transmission de données à caractère personnel à des tiers

SK ne divulgue ni ne transmet des données à caractère personnel à des tiers à l'exception des cas suivants :

- Une telle obligation découle de la législation applicable ou de mesures adoptées sous celle-ci (par ex. transmission vers une autorité d'enquête) ;
- Ces tiers sont impliqués dans la prestation des services ;
- Le tiers a un intérêt légitime à demander les données à SK ;
- SK a le droit, à des fins d'exécution d'un contrat ou pour assurer la performance d'un contrat, de transmettre les données à des tiers, y compris des entreprises de collecte de dettes et d'information de crédit et à d'autres personnes gérant des réclamations de dettes, ainsi qu'à des conseillers juridiques et des huissiers si la personne concernée n'a pas respecté le contrat ;
- La personne concernée fournit son consentement, par écrit, à la divulgation des informations à des tiers.

SK confirme qu'elle transmettra des données à caractère personnel uniquement dans la stricte mesure nécessaire et pour les finalités pour lesquelles les données à caractère personnel sont traitées.

SK divulgue vos certificats Estoniens valides associés à vos documents d'identité (y compris une Mobile-ID délivrée jusqu'au 02.07.2022) pendant leur période de validité par l'intermédiaire du service LDAP. Plus d'informations à propos du service LDAP est disponible [ici](#).

## 12. Période de stockage des données à caractère personnel

SK traite les données à caractère personnel aussi longtemps que nécessaire pour remplir les fonctions pour lesquelles les données à caractère personnel ont été collectées ou pour satisfaire les obligations émanant de la législation applicable. Veuillez noter qu'afin de fournir des services de confiance, nous sommes guidés par le règlement Eidas et les services de confiance et d'identification électronique d'Estonie relatifs à la loi sur les transactions électroniques à l'égard du stockage des données à caractère personnel.

SK est dans l'obligation de retenir des preuves utilisées pour vous identifier lors de l'émission de certificats pendant une période d'au moins 10 ans après la date d'expiration d'un certificat et des journaux associés à la procédure exécutée pendant la fourniture de services de confiance pendant au moins 10 ans afin de prouver tout mauvais usage de votre identité et le caractère approprié des opérations de SK en ce qui concerne la prestation de ses services, le cas échéant. La rétention des données et des preuves est requise par la loi et vérifiée par des auditeurs et organismes de contrôles indépendants.

## 13. Cookies

SK utilise des cookies sur ses sites web. Les cookies sont utilisés sur la base des politiques relatives aux cookies sur les sites web qui sont disponibles sur le [Site web de SK](#).

## 14. Amendement des principes de traitement des données à caractère personnel

SK se réserve le droit de modifier unilatéralement ces principes de traitement de données à caractère personnel conformément aux exigences établies par la législation applicable. Les amendements seront publiés sur le [Site web de SK](#) et entreront immédiatement en vigueur.