LA CHARTE PRIVACY

ETHIAS SA

La bonne gestion de vos données, notre priorité

Table des matiières

Préambule

En 2016, la Commission européenne a adopté le Règlement général sur la protection des données (ci-après « GDPR »). Elle instaure dès lors un **cadre législatif uniformisé** à l'ensemble du territoire de l'Union Européenne en ce qui concerne le traitement des données à caractère personnel. Le GDPR répond principalement à un double objectif : **responsabiliser les organismes qui traitent les données** et **renforcer les droits** des personnes dont les données sont traitées.

Le GDPR est entré en vigueur le 25 mai 2018 et s'applique à toute organisation ou entreprise qui traite des données à caractère personnel pour son compte ou non, dès lors qu'elle est établie dans l'Union Européenne ou que son activité cible directement les résidents européens. Le GDPR est donc applicable à Ethias S.A.

Chez Ethias S.A. (ci-après « Ethias » ou « nous »), nous mettons tout en œuvre pour assurer le **respect de votre vie privée** et la **protection de vos données à caractère personnel**. La « protection des données dès la conception » (ci-après « privacy by design ») est également une priorité au sein de notre entreprise. Ce principe signifie que la protection des données est prise en compte dès la phase initiale du développement de nos projets et de nos produits mais également, tout au long de leurs évolutions.

Nous traitons vos données à caractère personnel afin de pouvoir vous offrir un service optimal et adapté à vos besoins. Celles-ci sont traitées dans le **respect des finalités** pour lesquelles vous nous les avez confiées et en toute **transparence**.

Dans le souci de souligner notre engagement en matière de vie privée, nous avons élaboré cette Charte relative à la protection des données (ci-après, la « Charte »). Celle-ci vise à vous informer des traitements qu'Ethias réalise, au travers de ses différentes marques (Ethias et Flora), de la manière dont Ethias protège vos données personnelles et des droits dont vous disposez.

Nous vous invitons à lire attentivement cette Charte qui souligne, par ailleurs, nos valeurs fondamentales, à savoir l'Humain et la Satisfaction du client. Pour toute autre question, n'hésitez pas à nous contacter à l'adresse suivante : DPO@ethias.be ou privacy_request@ethias.be si vous voulez exercer les droits que vous reconnaît le GDPR.

Nous attirons votre attention sur le fait que nos sites Internet peuvent parfois contenir des liens vers des sites de tiers (médias sociaux, organisateurs d'événements que nous sponsorisons, etc.) dont les conditions d'utilisation ne tombent pas sous le champ d'application de cette Charte ni sous notre responsabilité.
Nous vous recommandons par conséquent de lire attentivement leur Charte de protection des données à caractère personnel pour savoir comment ils respectent votre vie privée.

Charte relative à la protection des données

Ci-dessous, vous trouverez un aperçu des différents chapitres développés au sein de notre Charte.

Pour un accès rapide à un chapitre, cliquez sur le lien relatif au chapitre. Si vous souhaitez accéder à la Charte dans son entièreté, nous vous invitons à faire défiler le texte.

1. Règlement général sur la protection des données

Le GDPR est un Règlement européen qui vise à établir un cadre uniforme en matière de protection des données. Il est applicable au sein de tous les États Membres de l'Union Européenne depuis le 25 mai 2018.

En droit belge, il existe une loi qui vient compléter et préciser certaines dispositions du GDPR. Il s'agit de la loi du 30 juillet 2018, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.

A la fin de cette Charte (Voir infra, Chapitre 19), vous trouverez une **liste de définitions** utile à la compréhension des termes utilisés. Nous vous invitons à la parcourir et à vous familiariser avec son contenu.

2. A qui s'adresse cette Charte ?

Cette Charte est destinée aux **personnes physiques** dont Ethias est amenée à traiter les données à caractère personnel telles que :

- des prospects ou candidats-preneurs d'assurance;
- des personnes concernées par un contrat d'assurance (preneurs d'assurance, assurés, bénéficiaires);
- des personnes impliquées dans un sinistre (parties préjudiciées, témoins, et leurs éventuels représentants);
- des différentes personnes appelées à intervenir lors de la conclusion d'un contrat d'assurance ou de la gestion d'un sinistre (intermédiaires d'assurances, experts médicaux, réparateurs, dépanneurs, prestataires de soins, etc.) ;
- des personnes qui soumettent leur candidature pour un poste vacant auprès d'Ethias ;
- des personnes qui ont un lien avec nos clients tels que les membres du personnel de ceux-ci ou leurs actionnaires.

Les données des personnes morales en tant que telles ne sont concernées ni par le GDPR ni par la présente Charte.

3. Responsable du traitement des données

Ethias S.A. (ci-après « Ethias » ou « nous ») est le responsable du traitement de vos données à caractère personnel qu'elle traite au travers de ses différentes marques (Ethias et Flora). Ethias est une société de droit belge, dont le siège social est situé voie Gisèle Halimi 10 à 4000 Liège, Belgique, enregistrée à la Banque Carrefour des Entreprises de Belgique sous le numéro 0404.484.654.

En qualité de responsable de traitement, nous déterminons les finalités (le « pourquoi ») et les moyens (le « comment ») du traitement de vos données à caractère personnel, et sommes votre interlocuteur principal (ainsi que celui des autorités de contrôle) pour toute question relative au traitement de celles-ci. La présente Charte vise à vous informer sur le traitement de vos données dont la responsabilité nous incombe.

Notre **délégué à la protection des données** (ci-après « DPD », « Data Protection Officer » ou « DPO ») est chargé du suivi de la politique en matière de protection des données. (le chapitre 4 est consacré à la question de la mise en place d'une structure de gouvernance vie privée au sein d'Ethias). Vous pouvez le contacter :

- par courrier à l'adresse suivante :
  Ethias SA - Data Protection Officer
  voie Gisèle Halimi 10
  4000 Liège
- par e-mail à l'adresse DPO@ethias.be.

4. Notre engagement

Nous mettons un point d'honneur à respecter votre vie privée et à traiter vos données à caractère personnel dans la plus stricte confidentialité et conformément à la législation en vigueur. C'est pourquoi nous avons mis en place de solides pratiques de gouvernance de données à caractère personnel. Cet engagement s'implémente notamment dans les mesures suivantes :

- **la tenue d'un registre de traitements des données à caractère personnel** lorsque nous agissons en qualité de responsable de traitement ;
- **la mise en place d'une structure de gouvernance vie privée au sein d'Ethias**. Nous avons désigné un Data Protection Officer. Comme expliqué ci-dessus, celui-ci est notre point de contact unique pour toutes questions relatives à la protection des données. Nous avons également mis en place un réseau de « collaborateurs GDPR » spécialement formés en matière de vie privée. Ces derniers sont déployés au sein des directions et départements : ils assurent le relais entre le DPO et les directions/départements, se chargent de la conformité GDPR et répondent aux questions spécifiques relatives à la protection des données ;
- **la mise en place d'un processus de gestion de projets garantissant le principe du « Privacy by design »**. L'objectif de celui-ci est d'assurer la conformité des projets en cours de développement et des traitements existants aux législations et bonnes pratiques privacy en vigueur. Pour tout nouveau projet ou produit d'Ethias, le réseau GDPR est impliqué dès le début. En outre, le DPO y exerce son contrôle ;
- **la réalisation d'analyse d'impact sur la protection des données** (ci-après « AIPD », « Data Protection Impact Assessment » ou « DPIA ») pour tout traitement de données présentant un risque élevé pour vos droits et libertés et, lorsque ce risque est avéré, l'élaboration et l'implémentation de mesures pour réduire ce risque. La réalisation de ces DPIAs vise à garantir qu'Ethias gère de manière adéquate les risques que posent les opérations de traitement « à risque » pour la protection des données et de la vie privée. En proposant une réflexion structurée sur les risques pour les personnes concernées et sur la manière de les atténuer, le DPIA nous aide à nous conformer à l'exigence de la « protection des données dès la conception » (« privacy by design »).

5. Données traitées

Nous traitons vos données en toute transparence pour les finalités spécifiées lors de leurs collectes.

Les données à caractère personnel traitées appartiennent aux catégories développées ci-dessous.

a. Données à caractère personnel

Cette catégorie se rapporte aux données qui permettent de vous identifier directement (par exemple votre nom ou prénom) ou indirectement (par ex. votre numéro de téléphone ou la plaque d'immatriculation de votre véhicule).

En fonction du type d'assurance que vous contractez, les données suivantes peuvent être collectées :

- données d'identification (nom, prénom, adresse, etc.) ;
- données de contact (adresse, adresse électronique, numéro de téléphone, etc.) ;
- composition du ménage (état civil, nombre d'enfants, etc.) ;
- vue financière globale (vos biens immobiliers, rémunération, contrats d'assurances etc.) ;
- caractéristiques du logement, du véhicule ;
- profession (fonction exercée, formation, etc.) ;
- loisirs et intérêts ; et
- des enregistrements d'images tels que des films, photos, enregistrements vidéos.

b. Données sensibles

Certaines données à caractère personnel, en raison de leur caractère particulièrement sensible, bénéficient d'une protection particulière. Il s'agit notamment d'informations qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Vos données sensibles ne sont en aucun cas traitées sans votre consentement préalable explicite lorsqu'il est requis. Elles ne sont jamais traitées à des fins de prospection.

c. Données relatives aux condamnations pénales et aux infractions

Nous ne traitons les données relatives aux condamnations pénales et aux infractions que dans les cas suivants :

- lorsqu'une loi prévoyant des garanties adéquates l'y autorise ;
- lorsque nous en avons besoin pour gérer nos propres contentieux ;
- lorsque vous nous avez donné votre consentement de manière explicite ;
- lors de conseils juridiques, pour autant que la défense de nos clients l'exige.

6. Moyens de collecte de vos données à caractère personnel ?

Nous collectons vos données à caractère personnel soit directement auprès de vous ou soit par l'intermédiaire d'un tiers.

a. Données collectées directement auprès de vous

Nous collectons vos données à caractère personnel directement lorsque par exemple :

- vous devenez client ;
- vous remplissez tout formulaire approprié que nous vous soumettons ;
- vous utilisez nos services et produits ;
- vous vous abonnez à nos newsletters, répondez à nos invitations (conférences, etc.), participez à nos concours, etc. ;
- vous nous contactez par les différents canaux de communication mis à votre disposition ;
- vos données sont transmises par des personnes que vous avez mandatées (assureurs, avocats, experts, membres de la famille etc.) ou qui sont autorisées à le faire en vertu d'une réglementation;
- vous êtes filmé par nos caméras de surveillance situées dans et aux abords de nos bâtiments. Les images sont enregistrées uniquement dans le but de préserver la sécurité des biens et des personnes ainsi que de prévenir les abus, fraudes et autres infractions dont nos clients et nous-même pourrions être victimes (leur présence est signalée par des autocollants munis de nos coordonnées de contact) ;
- vous communiquez des données lors de l'utilisation de nos sites Internet (y compris nos pages sur les réseaux sociaux) et de nos applications mobiles, par exemple lorsque :
  - vous nous communiquez vos données lors de la souscription à notre newsletter ;
  - vous demandez en ligne une offre d'assurance ;
  - vous remplissez vos données en ligne pour soumettre votre candidature pour un poste vacant auprès d'Ethias ;

- vous déclarez un sinistre ou vous demandez de l'assistance ;
- vous déclarez une hospitalisation ;
- vous souscrivez des contrats en ligne ;
- vous remplissez vos données dans les « zones privées » des sites Internet ;
- vous créez votre personnage Ethias ;

- vous visitez un de nos sites Internet ou vous utilisez une de nos applications mobiles qui contiennent des cookies et autres technologies similaires. Pour plus d'informations sur les cookies que nous utilisons, nous vous invitons à consulter notre Cookie Policy: https://www.ethias.be/part/fr/legal/cookie-infopage.html.

Lorsque nous vous demandons de nous communiquer des données à caractère personnel, vous avez le droit de ne pas y répondre. Ce refus pourrait toutefois empêcher la naissance de relations contractuelles, modifier la nature de celles-ci ou en influencer la gestion.

b. Données collectées par l'intermédiaire de tiers

Nous collectons vos données à caractère personnel **par l'intermédiaire de tiers** qui nous les ont communiquées dans le cadre de la souscription ou de la gestion d'un contrat ou de la gestion d'un sinistre ou dans le cadre de nos activités promotionnelles organisées conformément à la règlementation applicable en matière de e-privacy et de protection des données à caractère personnel.

C'est notamment le cas :

- d'un employeur qui souscrit pour le compte de son personnel une assurance de groupe, une assurance accident de travail une assurance collective soins de santé ;
- d'un établissement scolaire qui nous communique l'identité des personnes accidentées ou impliquées dans un sinistre ;
- d'une fédération sportive ou d'un club sportif qui nous communique l'identité des membres assurés et des personnes accidentées ou impliquées dans un sinistre ; et
- des parties impliquées dans un sinistre qui nous communiquent l'identité des parties adverses ou des témoins ; et
- des partenaires commerciaux d'Ethias dans le cadre des activités promotionnelles d'Ethias.

Nous collectons également vos données qui sont publiées (Moniteur belge).

7. Bases légales et finalités du traitement des données

Conformément au GDPR, chaque traitement de données s'appuie sur une **base légale** et répond à **une/des finalité(s)** spécifique(s).

Il est basé sur une seule base légale. Cette dernière est déterminée en fonction des éléments suivants :

- la nature des données à caractère personnel ; et
- la finalité spécifique (l'objectif ou le « pourquoi ») pour laquelle nous souhaitons traiter vos données.

a. Base légale : En vue de la conclusion, l'exécution et/ou de la gestion d'un contrat à votre demande :

Vos données peuvent être collectées pour :

- la gestion de la relation client ;
- l'évaluation de l'opportunité de conclure un contrat d'assurance et/ou des conditions à y assortir;
- la fourniture de services ;
- la gestion et le traitement de réclamations ;
- la préparation et la collecte des factures ;
- le suivi des discussions commerciales et des litiges avec nos clients et la réponse aux questions éventuelles ;
- la fourniture d'un soutien technique ;
- la gestion des contrats et des sinistres.

b. *Base légale : En vue de respecter les obligations, légales, réglementaires et administratives nous incombant en notre qualité d'assureur*

Vos données peuvent être collectées pour :

- la gestion des accidents du travail, assurance de groupe ou de pensions, prêt hypothécaire, prévention du blanchiment de capitaux et du financement du terrorisme ;
- la mise en œuvre de la législation Insurance Distribution Directive (IDD) ;
- la lutte contre la fraude fiscale ;
- l'exécution des obligations sociales et fiscales d'Ethias ;
- l'exécution de notre obligation de répondre aux questions des autorités de contrôle ou gouvernementales telles que l'Autorité de protection des données (APD), l'Autorité des services et marchés financiers (FSMA), la Banque Nationale de Belgique (BNB), les Organisations sectorielles ou de consommateurs (par ex. Ombudsman des Assurances), etc.

c. *Base légale : Lorsqu'il relève de notre intérêt légitime ou de celui de tiers (tels que nos assurés et créanciers)*

Dans cette hypothèse, nous procédons à une évaluation approfondie afin de maintenir un juste équilibre entre notre intérêt légitime ou celui du tiers et le respect de votre vie privée.

Vos données peuvent être collectées pour :

- la détection et la prévention des abus et fraudes et la gestion des recours qui pourraient être intentés par Ethias;
- la protection des biens de l'entreprise ;
- la sécurité des biens et des personnes, ainsi que de nos réseaux et systèmes informatiques ;
- la sauvegarde de nos intérêts propres et à ceux de nos assurés ;
- la révélation de tout abus portant ou susceptible de porter un préjudice sérieux à notre statut financier, nos résultats et/ou à notre réputation ;
- la constitution de preuve(s) ;
- le suivi de nos activités et la connaissance administrative des différentes personnes liées à Ethias, qui permet l'identification des dossiers, de l'intermédiaire et d'autres intervenants ;
- la réalisation d'enquêtes de satisfaction ;
- une candidature que vous soumettez en communiquant à Ethias vos données en ligne ;
- la gestion des fichiers clients afin d'avoir une vision plus globale (par ex. l'établissement de statistiques en vue de savoir qui sont nos clients et comment les connaitre davantage) ;
- la réalisation de tests évaluation des risques, simplification, optimalisation et/ou automatisation ;
- la mise en œuvre de processus purement internes à Ethias afin de les rendre plus efficaces ;
- la mise en œuvre de systèmes en ligne afin d'améliorer votre expérience en tant qu'utilisateur (par ex. résoudre des bugs sur nos sites Internet et applications mobiles, vous contacter pour résoudre des problèmes techniques lorsque nous avons constaté que vous avez commencé à remplir vos données en ligne pour bénéficier d'un service mais que vous n'avez pas pu continuer ce processus, etc.) ;
- l'optimisation et la gestion des canaux de distribution d'Ethias.

*Sur base de notre **intérêt légitime**, nous pouvons traiter vos données à caractère personnel à des fins de prospection*

Sauf opposition de votre part, nous sommes susceptibles de vous adresser des offres :

- par courrier ordinaire, par téléphone ;
- par voie électronique pour nos produits et services similaires à ceux auxquels vous avez déjà souscrits.

Nous nous assurons que ces offres commerciales aient une plus-value par rapport aux produits et services dont vous bénéficiez déjà afin de nous assurer du juste équilibre entre nos intérêts respectifs.

En aucun cas, nous n'utilisons vos données sensibles (à savoir celles visées au Chapitre 5, point b) et c), telles que vos données santés) dans le cadre de la prospection. En outre, en l'absence d'un consentement préalable de votre part, nous ne transférons et ne communiquons pas vos données à des tiers pour leurs propres prospections.

Nous n'adressons pas de publicité relative à des produits d'assurance directement aux mineurs de moins de 16 ans sauf en cas de consentement donné par le titulaire de la responsabilité parentale.

d. *Base légale : Lorsque nous vous avons demandé votre consentement et que vous (ou votre représentant légal) nous l'avez donné*

Dans ce cas, vos données à caractère personnel sont traitées pour la ou les finalité(s) spécifique(s) auxquelles vous avez consentie(s) via nos documents contractuels, nos formulaires-type, ou des intermédiaires d'assurance.

Nous vous rappelons que vous pouvez retirer votre consentement à tout moment.

Nous demanderons en particulier votre consentement :

- afin d'optimiser le portefeuille des assurances que vous avez souscrites ;
- afin de bénéficier de la tarification la plus avantageuse ;
- afin de vous proposer des produits d'assurances plus adaptés à votre situation familiale ou professionnelle grâce à un profilage plus sophistiqué permettant de mieux anticiper vos comportements et vos besoins ;
- pour toute offre par voie électronique concernant des produits ou services non similaires à ceux auxquels vous avez déjà souscrits ;
- pour la communication de vos données à des tiers à des fins commerciales.

e. *Base légale : Lorsque nous vous avons demandé votre consentement **explicite***

Vos données sensibles peuvent être collectées, notamment, pour :

- la gestion de contrats d'assurances (assurance-vie, hospitalisation, soins de santé, revenu garanti, etc.), d'un sinistre avec dommage corporel ou de votre dossier médical (accident de roulage, du travail, sportif etc.) en ce qui concerne les données relatives à la santé ; et/ou
- afin de vous représenter dans le cadre d'assurances liées à votre activité professionnelle (par ex. assurance de groupe, accident du travail, etc.) lorsque vous mandatez un délégué syndical.
- L'évaluation de l'opportunité de conclure un contrat d'assurance auto et/ou des conditions à y assortir.

f. *Base légale : Lorsque le traitement est nécessaire à la constatation, l'exercice ou la défense d'un droit en justice. / Gestion de nos propres contentieux*

Nous pouvons être amenés à devoir traiter vos données à caractère personnel, y compris vos données de santé et/ou vos données à caractère personnel relatives aux condamnations pénales et aux infractions pour les cas suivants : soit pour la constatation, l'exercice ou la défense d'éventuels droits en justice, soit pour la gestion de nos propres litiges, lors de conseils juridiques, pour autant que la défense de nos clients l'exige.

8. Minimisation et proportionnalité

Seules les données à caractère personnel **adéquates**, **pertinentes** et **limitées** à ce qui est nécessaire par rapport aux finalités pour lesquelles elles sont traitées (principe de minimisation) sont collectées. Pour chaque traitement de données, nous vérifions si celui-ci est nécessaire pour atteindre la finalité visée et déterminons s'il s'agit de la mesure la moins intrusive par rapport aux autres moyens permettant de réaliser le même objectif.

9. Transparence

Nous mettons tout en œuvre pour vous fournir des informations **concises** et **claires** quant aux traitements de données effectués et à leurs finalités. Nous adaptons la langue, les termes et le moyen de communication utilisés en fonction du public visé.

10. Vos droits

Hormis les cas où le GPDR ou toute disposition légale en vigueur en Belgique s'y opposent, vous disposez des droits suivants :

- droit d'accès ;
- droit de rectification ;
- droit à l'effacement (« droit à l'oubli ») ;
- droit à la limitation de traitement ;

- droit à la portabilité de vos données ;
- droit à l'opposition, notamment à la prospection commerciale ;
- droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé y compris le profilage, produisant des effets juridiques vous concernant ou vous affectant de manière significative de façon similaire ;
- droit de retirer votre consentement.

Nous mettons en place des procédures qui vous permettent d'exercer efficacement vos droits liés au traitement des données à caractère personnel. Ces procédures visent également à assurer le traitement de vos demandes dans les meilleurs délais. En tant qu'assureur, Ethias ne peut prendre le risque de donner suite à une demande qui n'émanerait pas d'une personne autorisée. C'est pourquoi, nous devons vérifier l'identité de notre interlocuteur et vous demandons de nous communiquer une copie recto-verso de votre carte d'identité.

Pour **exercer vos droits**, nous vous invitons à nous communiquer votre demande datée et signée accompagnée d'une copie recto-verso de votre pièce d'identité par courrier à l'adresse suivante : Ethias SA, DIM-Spoc GDPR , voie Gisèle Halimi 10 à 4000 Liège ou par e-mail: privacy_request@ethias.be.

a. *Droit d'accès*

Vous avez le droit d'accéder à vos données à caractère personnel qui sont en notre possession.
Ce droit vous :

- la finalité du traitement des données ;
- les catégories de données à caractère personnel traitées ;
- les destinataires auxquels vos données sont communiquées ;
- lorsque cela est possible, leur durée de conservation, ou le cas échéant, les critères utilisés pour déterminer cette durée ;
- l'existence d'une prise de décision automatisée (y compris le profilage) et dans ce cas, la logique sous-jacente, ainsi que de l'importance et des conséquences de cette décision.

Notez que pour tout accès relatif à des données médicales, le délai pour en recevoir l'accès est d'un mois à partir de la réception de la demande ou de deux mois si les données demandées remontent à plus de 5 ans.

b. *Droit de rectification*

Il est primordial que vous conserviez la maitrise de vos données. Dès lors, si vous constatez que les données en notre possession sont inexactes, vous pouvez à tout moment nous demander de les compléter ou de les rectifier.

Après votre confirmation des changements apportés, veuillez compter un délai d'un mois à partir de la vérification de votre identité pour que vos données soient mises à jour.

c. *Droit à l'effacement (« droit à l'oubli »)*

Vous avez le droit de demander la suppression des données à caractère personnel en notre possession.
La loi prévoit les cas pour lesquels le droit à l'oubli peut être exercé, il s'agit notamment des cas suivants :

- vos données ne sont plus nécessaires au regard des finalités pour lesquelles nous les avons collectées ;
- le traitement de vos données est fondé exclusivement sur votre consentement et vous décidez de retirer celui-ci ;
- vous êtes opposé au traitement de vos données et il n'existe pas dans notre chef de motifs légitimes impérieux qui prévalent sur les vôtres ;
- vous estimez que le traitement est illicite et le fait est avéré.

Ce droit n'est toutefois pas absolu. Nous pouvons conserver vos données lorsque celles-ci sont nécessaires :

- à l'exécution d'une obligation légale ;
- à l'exécution de nos obligations contractuelles ;
- à des fins statistiques étant entendu que dans ce cas, nous prenons toutes les mesures techniques et organisationnelles pour assurer le respect du principe de minimisation des données ;
- à la constatation, à l'exercice ou à la défense de droits en justice.

Après votre confirmation de supprimer vos données en notre possession, veuillez compter un délai d'un mois maximum à partir de la vérification de votre identité pour que vos données soient supprimées.

d. Droit à la limitation du traitement

La loi prévoit les cas dans lesquels vous pouvez demander la limitation du traitement de vos données à caractère personnel. Il s'agit des hypothèses suivantes :

- vous contestez l'exactitude des données à caractère personnel, pendant une durée nous permettant de vérifier l'exactitude ou non des données ;
- le traitement est illicite et vous vous opposez à leur effacement et exigez à la place une limitation de leur utilisation ;
- vous constatez que vos données à caractère personnel ne nous sont plus nécessaires et souhaitez en limiter le traitement à la constatation, l'exercice ou la défense de vos droits en justice ;
- vous vous êtes opposé au traitement de vos données à caractère personnel lors de la vérification portant sur le point de savoir si nos motifs légitimes de poursuivre le traitement prévalent sur les vôtres.
  Dans ces hypothèses, notez que le traitement de vos données peut tout de même avoir lieu si :
  - vous consentez à ce traitement ; ou
  - le traitement de vos données est nécessaire à la constatation, l'exercice ou la défense de droits en justice ; ou
  - le traitement est nécessaire à la protection des droits d'une autre personne physique ou morale ; ou
  - le traitement est nécessaire pour des motifs importants d'intérêt public.

e. Droit à la portabilité

Lorsque vos données à caractère personnel sont traitées sur base de votre consentement ou parce qu'elles sont nécessaires à l'exécution d'un contrat, vous bénéficiez d'un droit à la portabilité. Ce dernier vous permet de récupérer une partie de vos données à caractère personnel dans un format structuré, couramment utilisé et lisible par machine. De plus, ce droit vous permet de nous demander à ce que vos données soient transmises à un autre responsable de traitement à condition toutefois que cette opération soit techniquement possible.

f. Droit d'opposition

Lorsque nous traitons vos données à caractère personnel sur base de notre intérêt légitime, vous avez l e droit de vous opposer à ce traitement sous réserve de raisons tenant à votre situation particulière.
Nous pouvons refuser votre demande d'opposition lorsque des motifs légitimes et impérieux nous imposent de poursuivre le traitement ou lorsque celui-ci est justifié pour la constatation, l'exercice ou la défense de droits en justice.

Notez que vous avez toujours le droit de vous opposer au traitement de vos données à caractère personnel au profilage ou à des fins de prospection ou marketing direct.

g. Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé y compris le profilage, produisant des effets juridiques vous concernant ou vous affectant de manière significative de façon similaire

Afin de vous offrir un service de qualité, nous automatisons certains traitements de données afin de faciliter la prise de décision. Ces traitements automatisés doivent répondre à des conditions strictes, ils doivent être soit :

- nécessaires à la conclusion ou à l'exécution du contrat ;
- basés sur votre consentement explicite ;
- légalement autorisés.

Au regard de cette décision automatisée, vous bénéficiez des droits suivants :

- être informé qu'une décision entièrement informatisée produisant des effets juridiques vous concernant ou vous affectant de manière significative de façon similaire a été prise à votre encontre ;
- demander et être informé de la logique qui sous-tend une telle décision, sa signification et les conséquences qui en découlent ;
- de contester la décision et d'exprimer votre point de vue ;
- de demander l'intervention d'un être humain pour le réexamen de la décision.

h. Droit de retirer votre consentement

Lorsque le traitement de vos données à caractère personnel est exclusivement basé sur votre consentement, vous pouvez décider de le retirer à tout moment. Nous nous assurerons que les données soient supprimées sauf si un autre motif juridique nous permet de les traiter (par ex. lorsque le traitement est nécessaire pour honorer un contrat).

Si les données supprimées sont traitées pour différentes finalités, nous ne pouvons pas utiliser ces données pour la partie du traitement pour laquelle votre consentement a été retiré, ni pour aucune des finalités, selon la nature du retrait de votre consentement.

Notez toutefois que lorsque votre demande porte sur des données relatives à la santé, celles-ci sont indispensables à la détermination de l'ampleur de l'indemnisation dans le cadre d'une demande d'intervention. En conséquence, nous pourrons nous trouver dans l'impossibilité de donner suite à votre demande ou d'appliquer le contrat.

De plus, l'exercice de ce droit ne remet pas en cause la légalité du traitement de vos données à caractère personnel effectué durant la période précédant votre demande.

i. Droit de réclamation

Si vous estimez que le traitement de vos données à caractère personnel constitue une atteinte à votre vie privée, vous avez également le droit d'introduire une plainte auprès de l'Autorité de protection des données (ci-après « APD ») :

- via leur site internet : www.autoriteprotectiondonnees.be
- par courrier à l'adresse suivante :

  Autorité de protection des données
  Rue de la Presse 35
  1000 Bruxelles
  Tél : +32 2 274 48 00
- par mail : contact@apd-gba.be

j. Exceptions à l'exercice de vos droits : dispositions particulières en matière de blanchiment d'argent

Conformément aux dispositions relatives au blanchiment d'argent, nous sommes tenus de prévenir, détecter et signaler les opérations de blanchiment d'argent aux autorités. Nous traitons à cet effet les données à caractère personnel que vous nous avez communiquées ainsi que celles de canaux tels que World-Check de Thomson Reuter ou d'autres moteurs de recherche en ligne. À la suite de ce traitement, nous pouvons être amenés à **bloquer** certaines transactions et à les signaler à la Cellule de Traitement des Informations Financières (CTIF). Les **droits mentionnés ci-dessus ne peuvent alors pas être exercés** et nous vous invitons à vous adresser à l'APD.

11. Conservation des données

Vos données à caractère personnel sont uniquement conservées **pendant la durée nécessaire à la réalisation de ces finalités**, en général vos données sont conservées jusqu'à la fin de l'exécution de votre contrat ou du sinistre et parfois au-delà comme expliqué ci-après. La durée de conservation varie selon le type de données et les législations applicables en la matière. Au-delà de cette durée, vos données sont supprimées.

Certaines de vos données sont cependant conservées en vue :

- de répondre à nos obligations légales de conservation ;
- de répondre à nos obligations découlant de législations sociales ;
- d'assurer l'exécution de réclamations contractuelles jusqu'à l'expiration du délai de prescription applicable ;
- de répondre à tout litige potentiel ou réel.

Le stockage de vos données implique des risques. Certains moyens peuvent être mis en œuvre en vue de limiter la conservation de celles-ci à savoir :

- restreindre les droits d'accès normaux aux données stockées ;
- moyens dédiés de stockage/archivage des données ;
- ségrégation des données ;
- utilisation de techniques de chiffrement ou cryptage, les données stockées seront inaccessibles via les paramètres standard des droits d'accès utilisateur et pour toutes opérations de traitement.

Nous veillons à ce que ces exigences de conservation soient également respectées par nos partenaires et fournisseurs qui traitent des données à caractère personnel en notre nom (nos sous-traitants).

Pour obtenir plus d'informations sur la durée de conservation de vos données à caractère personnel, nous vous invitons à vous adresser à l'adresse électronique suivante: DPO@ethias.be.

12. Transferts de données et destinataires

En tant qu'assureur, nous sommes contraints de communiquer vos données à caractère personnel à des tiers afin de mener à bien nos missions, de répondre aux demandes d'indemnisations de parties sinistrées, de respecter nos obligations légales ou dans le cadre de nos activités promotionnelles. Ces tiers peuvent être implantés au sein de l'Espace Economique Européen (ci-après « EEE ») mais également en dehors de celui-ci.

a. Transferts de données au sein de l'EEE – Destinataires

Au sein de l'EEE, vos données à caractère personnel peuvent être communiquées :

- à nos collaborateurs et conseillers ;
- aux autres entités du groupe, leurs collaborateurs et conseillers ;
- à d'autres entreprises d'assurances intervenant dans la gestion de contrats ou de sinistres, à leurs représentants en Belgique et à leurs correspondants à l'étranger ;
- à « Datassur »;
- aux entreprises de réassurance ;
- aux banques ;
- à des bureaux de règlement de sinistres (nationaux ou internationaux) ;
- dans certains cas, aux intermédiaires d'assurance avec lesquels nous collaborons ;
- à tous les experts médicaux ou techniques, avocats, conseils techniques, réparateurs, intervenant dans le cadre de la gestion d'un contrat ou d'un sinistre ;
- aux détectives privés pour les éventuelles enquêtes en matière de fraude ;
- à nos prestataires de services informatiques (NRB, Assurcard, etc.) ;
- à nos partenaires commerciaux (sous réserve de votre consentement) comme par exemple des associations de consommateurs, assurances.be, Ethias Services, etc. ;
- aux bureaux de marketing et de communication ;
- aux entreprises en charge de la gestion documentaire (scanning, archivage, expédition de courriers, etc.) ;
- aux autorités sociales, fiscales, administratives déterminées par la loi ;
- aux autorités de contrôle et à l'ombudsman des assurances.

Conformément aux pratiques usuelles en matière de sécurité et de protection des données, nous veillons à **ne transférer que les données nécessaires** à l'exercice de leurs tâches, à l'exécution d'une obligation contractuelle/légale, ou au regard de l'intérêt légitime qui justifie ce transfert. Ces tiers se sont également engagés auprès de nous à traiter ces données confidentiellement et dans les limites de la finalité pour laquelle elles ont été transférées.

En ce qui concerne nos **sous-traitants**, nous contractons systématiquement avec chacun d'entre eux un contrat de traitements de données. Ceux-ci doivent respecter les principes repris dans cette Charte. Nous réalisons des **audits** afin d'assurer leurs conformités aux règles contractuelles et règlementaires applicables. Nos sous-traitants sont également tenus de répercuter vis-à-vis de leurs propres sous-traitants ces obligations de conformité.

Notez que pour la communication de vos données à des fins commerciales ne peut avoir lieu sans votre consentement.

b. Transferts de données au tiers à l'extérieur de l'EEE – Destinataires

Si nous devions transférer vos données personnelles en dehors de l'EEE, nous vérifions que le pays en question dispose du même niveau de protection que celui en vigueur au sein de l'EEE, que des garanties appropriées ont été mises en place (encryption, pseudonymisation, clauses contractuelles types,...), ou encore, que des dérogations peuvent être invoquées.

Dans le cas de la gestion des sinistres, en fonction des situations, nous pourrions être appelés à transférer des données personnelles hors EEE, afin d'assurer la bonne exécution de notre contrat avec notre client.

13. Cookies

Nous utilisons des cookies sur nos sites internet.

Pour en savoir plus sur notre Politique en matière de cookies, nous vous invitons à consulter la page suivante : https://www.ethias.be/part/fr/legal/cookie-infopage.html.

14. Formation et sensibilisation

Sensibiliser notre personnel à la protection des données et aux principes du GDPR est une mission qui nous tient à cœur. Raison pour laquelle, nos employés bénéficient d'un programme de formations adapté à leurs fonctions et aux opérations de traitement de données qu'ils mènent.

De plus, notre réseau collaborateurs GDPR (voir ci-dessus « Sections 3 et 4 ») assure la sensibilisation du personnel et la promotion de la protection de la vie privée au sein de chacun de nos départements.

15. Sécurité et gouvernance: mesures techniques et organisationnelles

En termes de sécurité, nous implémentons des **mesures techniques et organisationnelles appropriées** afin de nous protéger contre la destruction, la perte, l'altération, la divulgation non-autorisée ou l'accès aux données à caractère personnel transmises, stockées ou traitées.

Afin de définir le niveau de sécurité adéquat pour notre organisation, nous évaluons les risques liés à chacun des traitements de données que nous opérons en fonction de leurs contextes (nature, finalité, portée, catégories de données traitées) et des moyens technologiques disponibles.

En termes de **gouvernance**, nous adoptons les procédures nécessaires pour veiller à l'accomplissement des obligations et exigences du GDPR à savoir :

- les analyses d'impact sur la protection des données (AIPD) ou Data Protection Impact Assessment (DPIA) ;
- les méthodologies d'évaluation des risques, notamment dans le cadre de transferts hors EEE (« Transfer Impact Assessments » ou « TIA ») ;
- les méthodologies de protection des données dès la conception et par défaut (« Privacy par design and Privacy par défaut »).

Ces procédures nous permettent de déterminer si le traitement des données est légal, si celui-ci présente des risques et si tel est le cas, les mesures techniques et organisationnelles à mettre en place pour réduire ces risques.

16. Modification de la Charte

Cette Charte peut être mise à jour à tout moment et sans avis de modification. Nous vous invitons à la consulter régulièrement sur notre site internet.

Dernière mise à jour : 02/04/2024.

17. Définitions

Termes	Définitions
Analyses d'impact sur la protection des données (AIPD)/ Data Protection Impact Assessment (DPIA)	Une analyse d'impact sur la protection des données est une étude qui doit être menée lorsqu'un traitement de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.
Autorité Protection des données (APD)	L'Autorité publique indépendante chargée de contrôler l'application des lois et règlements applicables en matière de protection des données.
Cookies	Un cookie est un petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine web (c'est-à-dire dans la majorité des cas à l'ensemble des pages d'un même site web). Ce fichier est automatiquement renvoyé lors de contacts ultérieurs avec le même domaine. Il peut permettre d'identifier une personne physique sur base des données personnelles qu'il collecte.

Termes	Définitions
Délégué à la protection des données (DPD)/ Data Protection Officer (DPO)	Le délégué à la protection des données, data protection officer ou « DPO » est chargé de mettre en œuvre la conformité au GDPR au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme. Dans certains cas, sa désignation est obligatoire.
Données à caractère personnel ou données - personnelles	Les données à caractère personnel sont des données se rapportant à une personne physique identifiée ou identifiable par la combinaison d'informations.
Données sensibles	Les données sensibles sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
Intérêt légitime	L'intérêt légitime est une des bases légales prévues par le GDPR sur laquelle peut se fonder un traitement de données personnelles. Le recours à cette base légale suppose que les intérêts (commerciaux, de sécurité des biens, etc.) poursuivis par l'organisme traitant les données ne créent pas de déséquilibre au détriment des droits et intérêts des personnes dont les données sont traitées.
Minimisation (Principe de)	Le principe de minimisation prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.
Personne concernée	Toutes les personnes physiques dont Ethias est amené à traiter les données.
Profilage	Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à un individu, notamment pour analyser ou prédire son comportement.
Responsable du traitement	Une personne physique ou morale (comme Ethias) qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.
Tiers	Un tiers est une toute personne (physique ou morale), autorité publique, ou autre organisme autorisé à traiter les données à caractère personnel.

Ethias sa voie Gisèle Halimi 10 4000 Liège www.ethias.be info@ethias.be

Entreprise d'assurances agréée sous le n° 0196 pour pratiquer toutes les branches d'assurances Non Vie, les assurances sur la vie, les assurances de nuptialité et de natalité (AR des 4 et 13 juillet 1979, MB du 14 juillet 1979) ainsi que les opérations de capitalisation (Décision CBFA du 9 janvier 2007, MB du 16 janvier 2007).
RPM Liège TVA BE 0404.484.654 Compte Belfius Banque : BE72 0910 0078 4416 BIC : GKCCBEBB

1035-Charte Privacy_FR • 03/25