

Déclaration concernant la protection des données à caractère personnel des clients, fournisseurs d'itrust consulting s.à r.l. (ITR-DéclProtectClients)

1 Informations générales

Dernière mise à jour	18/06/2024
Engagement d'itrust consulting	Respecter la vie privée de tout un chacun, tel est l'objectif poursuivi par itrust consulting qui s'engage à veiller à la protection de vos données à caractère personnel. itrust consulting souhaite vous informer en toute transparence sur la manière dont elle collecte, utilise et protège vos données à caractère personnel et met en œuvre des moyens adéquats pour assurer la protection de vos données et la conformité aux exigences.
Domaine d'application	Cette déclaration de protection des données s'applique à toutes les données personnelles transmises à itrust consulting et celles que d'itrust consulting est amenée à traiter dans le cadre de ses activités. Elle ne couvre pas les données du personnel.
Responsable du traitement	La société itrust consulting est responsable de vos données à caractère personnel et assure le respect de la réglementation. Vous pouvez contacter itrust consulting ou son gérant à l'adresse suivante Carlo Harpes, info@itrust.lu , +352 26 17 62 12. En outre, itrust consulting a nommé un délégué à la protection des données (DPO) pour vous aider à faire valoir vos droits.
Contact DPO	Guillaume Schaff, dpo@itrust.lu , +352 621 699 975.
Modification	itrust consulting peut modifier cette déclaration sur le respect de la vie privée en publiant une version mise à jour sur notre site web.

2 Principes d'itrust consulting

itrust consulting confère une grande importance à la protection des données personnelles et au respect de la vie privée. Ceci est confirmé par la mise en application d'une politique de protection des données propre à itrust consulting.

Ainsi, la démarche d'itrust consulting est basée sur six principes :

1. itrust consulting utilise toujours vos données personnelles de façon loyale et digne de confiance.
2. Il s'engage à prendre toutes les mesures techniques et organisationnelles appropriées afin de protéger la sécurité de vos données à caractère personnel et principalement la confidentialité, l'intégrité et la disponibilité de vos données à caractère personnel.
3. Vous avez le droit d'être informé sur la façon dont vos données à caractère personnel sont utilisées. itrust consulting sera transparente envers vous sur les données qui sont collectées et sur la manière dont elles sont utilisées.
4. Si vous avez des incertitudes quant à la façon dont vos données personnelles sont traitées, veuillez nous contacter afin que nous puissions répondre à vos questions dans les meilleurs délais.
5. Toutes les mesures nécessaires sont prises afin de protéger vos informations contre les abus et les conserver en toute sécurité.
6. itrust consulting coopère avec la Commission nationale pour la Protection des Données (ci-après, la CNPD), ayant son siège à L-4361 Esch-sur-Alzette, 1 avenue du Rock'n'roll.

3 Règles de conduite d'itrust consulting

3.1 Quelle est la mission d'itrust consulting ?

Vos données à caractère personnel sont utilisées uniquement dans le cadre de la mission d'itrust consulting, qui est spécialisée dans les systèmes de sécurité de l'information et aide ses clients des secteurs public et privé à protéger leurs informations contre toute divulgation, manipulation ou indisponibilité. Elle consiste à offrir des services liés à :

- l'élaboration, l'implémentation et l'audit des systèmes de gestion de la sécurité de l'information ;
- l'évaluation et le traitement du risque à l'aide de son outil TRICK Service ;
- le déploiement de ses experts de sécurité en cas de besoin (SECaaS, la sécurité en tant que service) ;
- le piratage sur demande de nos propres clients et la gestion des incidents de cybersécurité (malware.lu CERT) ; ou encore
- la mise en place et le pilotage de solutions de sécurité pour l'ICT.

Vous trouverez plus de détails sur le site <http://www.itrust.lu>.

3.2 Quelles sont les finalités des traitements ?

La collecte et le traitement de vos données à caractère personnel se limitent aux finalités suivantes :

- Gérer les données conformément au contrat (conseil, audit, formation, recherche, ...).

- Attribuer des noms de connexion ou des pseudonymes aux étudiants qui effectuent des tests standardisés ; permettre l'accès au lien à l'enseignant qui supervise le test et fournit un retour d'information aux étudiants.
- Traduire des ensembles de noms d'étudiants ayant des propriétés similaires en classes de pseudonymes afin d'effectuer une corrélation statistique des résultats des tests avec ces propriétés, sans révéler l'identité des participants aux tests.
- Démontrer la qualité du travail ou identifier les erreurs en cas de réclamation (par le client ou les parties prenantes).
- Réutiliser le savoir-faire appliqué à un client pour un autre.
- Documenter l'histoire de l'InfoSec et de la CyberSec au Luxembourg.
- Proposer des services généraux et sur mesure, inscrire les clients en établissant des contrats, modifier les contrats.
- Facturer les clients et assurer le suivi des paiements et de la clôture des projets.
- Gérer les actions du personnel sur tous les systèmes informatiques.
- Assurer la sécurité des systèmes informatiques.
- Contrôler le personnel et assurer la sécurité sur le lieu de travail.
- Gérer et payer les salaires et les charges sociales.
- Gérer les informations comptables conformément aux exigences légales.
- Préparer ou soutenir les décisions de gestion interne.
- Assister les clients dans leurs activités d'analyse médico-légale et d'équipe d'intervention en cas d'événement.
- Héberger la base de données des logiciels malveillants, les outils de test des logiciels malveillants et gérer les connaissances techniques liées aux logiciels malveillants.
- Simplifier la navigation sur le site web.
- Assurer la sécurité des systèmes informatiques, c'est-à-dire prouver que personne n'a touché aux systèmes informatiques d'itrust.
- Enquêter sur les manipulations.

3.3 Qui est concerné par le traitement de données ?

Sont concernés :

- tous les clients, en particulier le personnel des clients communiquant avec itrust consulting ;
- tous les partenaires contractuels et sous-traitants ;
- les étudiants et les enseignants concernés par la gestion d'ÉpStan ;
- tous les employés d'itrust consulting.

3.4 Comment vos données à caractère personnel sont-elles collectées ?

Concernant les personnes citées au point 3.3, les données sont collectées à partir

- a. les informations que vous nous donnez directement ;

- b. les informations que nous pouvons recueillir par le biais de nos activités de navigation sur nos sites « web itrust.lu » et « malware.lu », et que nous pouvons recueillir sur des sources comme LinkedIn, twitter, etc ;
- c. Base de données gérant ÉpStan.

3.5 De quelles données à caractère personnel dispose itrust consulting ?

Comme « données à caractère personnel », sont considérées les informations qui permettent de vous identifier ou de vous rendre identifiable. Il peut s'agir notamment :

- vos nom, adresse, identifiants, image de profil, adresse électronique et numéro de téléphone ;
- des informations électroniques (adresse IP, informations de navigation) ;
- d'autres informations sur vos activités commerciales passées ou actuelles, ainsi que des informations, y compris des IIP, que vous pourriez nous transmettre ;
- les évaluations des employées ;
- les informations relatives aux mesures disciplinaires.

3.6 Quelle est la durée de conservation des données ?

Vos données à caractère personnel sont conservées pour la durée nécessaire à la réalisation des finalités susmentionnées.

Ces délais peuvent toutefois être augmentés par la nécessité d'appliquer des délais de prescription légaux. Les durées de conservation ont été définies dans le registre des traitements et peuvent être consultées dans les locaux d'itrust consulting. En tant que client, vos données personnelles ne sont conservées par itrust consulting uniquement pendant la période de relation d'affaire. Pour toute question quant à la durée de rétention de vos données, vous pouvez contacter notre DPO.

Selon la finalité ou les dispositions des lois sur l'archivage, la durée de conservation pourrait être étendue. En effet, certaines images sont conservées et utilisées à des fins historiques.

Sous forme anonymisée, vos données à caractère personnel pourront être exploitées à des fins statistiques au-delà de toute durée de conservation indiquée ci-devant.

La gestion des connaissances pour la fourniture de services commerciaux et la gestion des données clients enregistrées ou traitées est la suivante :

Type de donnée	Temps de rétention	Temps d'effacement après une requête.
Informations à caractère personnels isolés conservées comme preuve lors d'une mission de conseil ou d'audit.	10 ans à compter de la clôture de l'année sociale, sauf en cas de litige existant devant le tribunal civil. 30 ans (pour le commercial, il s'agit seulement de 10 ans après la clôture de l'année sociale de la décision judiciaire définitive.	1 mois

Documents papier liés au client.	3 ans après la fin du projet.	2 mois
Rapports de connexion et d'activité (liés aux activités du personnel du client, par exemple changements Owncloud, connexions app.trickservice, conférences MS Teams...)	0 ans (Il s'agit d'un maximum ; selon les systèmes, les journaux sont supprimés plus rapidement ou en cas de mise à niveau, par exemple dans MS Team, les journaux sont supprimés conformément aux politiques de MS).	2 mois
Journaux informatiques	5 ans (Max)	2 mois
Certains rapports de clients (qui n'ont pas fait l'objet d'une demande de suppression) peuvent être conservés à des fins scientifiques et journalistiques, par exemple le premier incident de logiciel malveillant discuté au Parlement luxembourgeois, la première analyse 27001 Gab dans le secteur public...).	30y	2 mois

Tableau 1: Durée de conservation de l'enregistrement des activités de traitement pour la gestion des données clients

3.7 Avec qui vos données à caractère personnel sont-elles partagées ?

En règle générale, vos données personnelles ne sont pas partagées en dehors d'itrust consulting. L'accès à vos données ne sera accordé qu'aux employés d'itrust consulting qui en ont besoin dans l'exercice de leurs responsabilités.

Dans le cadre d'enquêtes d'autres autorités (p.ex. enquête policière), itrust consulting pourra être amenée à leur fournir les informations nécessaires à leur enquête.

En cas de participation à des événements, nous transmettons avec votre accord les données nécessaires aux organisateurs.

Si nous traitons vos données, vous pouvez envoyer un email au DPO pour en savoir plus sur la liste de nos sous-traitants.

3.8 Vos données à caractère personnel sont-elles transférées vers des pays tiers (hors UE et pays partenaires) ?

Aucune de vos données à caractère personnel n'est transférée vers des organismes établis en dehors de l'UE.

3.9 Comment vos données à caractère personnel sont-elles protégées ?

L'accès à vos données à caractère personnel est restreint afin d'éviter tout accès non autorisé, modification ou utilisation abusive. Des accès sont octroyés uniquement aux membres du personnel qui en auraient besoin pour l'accomplissement de leur mission.

3.10 Comment itrust consulting gère les cookies

Un cookie est un fichier texte envoyé à votre navigateur et stocké sur le disque dur de votre appareil (par exemple, PC, ordinateur portable ou smartphone) lorsque vous visitez notre site web.

itrust consulting utilise différents types de cookies. Les cookies de session ou de préférence, qui sont essentiels pour la navigation et le bon fonctionnement du site. Les cookies de mesure d'audience, qui permettent de suivre les informations suivantes sur les visiteurs. L'objectif de ces cookies est de mesurer le nombre d'utilisateurs des services. Cookies à des fins statistiques pour suivre la façon dont les utilisateurs naviguent sur notre site. itrust utilise la solution Matomo, configurée selon les recommandations de l'EDPB pour se conformer au GDPR. Ces cookies ne contiennent aucune donnée personnelle.

itrust consulting conserve les données collectées par les cookies en les stockant dans les serveurs de données qui appartiennent à itrust consulting et qui sont situés au siège d'itrust consulting. Les données sont stockées en Europe.

Les cookies placés par notre site web ne peuvent être lus que par celui-ci. itrust consulting n'utilise pas de service externe pour analyser la façon dont les gens utilisent son site.

Nous utilisons des cookies pour évaluer la fonctionnalité de notre site web et pour collecter des données afin de créer des statistiques pour améliorer la qualité. Vous pouvez accepter ou refuser nos cookies (uniquement les cookies de statistiques). Une option par défaut "pas de consentement" s'applique au cas où vous n'auriez pas choisi. Si vous choisissez de refuser nos cookies, nous n'installerons pas de cookies statistiques, car les cookies fonctionnels sont toujours installés automatiquement. Si vous souhaitez en savoir plus sur notre politique en matière de cookies, veuillez cliquer sur le lien "Plus d'informations".

3.11 Quels sont vos droits et comment les exercer ?

Les règles légales en matière de protection des données à caractère personnel, notamment les droits reconnus aux personnes concernées par les traitements effectués sont applicables dans les conditions afférentes et sous réserve des exceptions et dérogations prévues.

Pour des questions relatives au traitement de vos données ou en vue de faire valoir l'exercice de vos droits, vous pouvez contacter le délégué à la protection des données d'itrust consulting,

- en lui adressant un courriel à l'adresse suivante : dpo@itrust.lu
- ou par courrier recommandé à :

itrust consulting s.à r.l.
Data Protection Officer
G. Schaff
55, rue Gabriel Lippmann
L-6947 Niederanven, LUXEMBOURG,

tout en joignant à votre demande une copie lisible et valable de votre pièce d'identité ainsi que, s'il y a lieu, de celle de la personne dont vous êtes le représentant légal.

En cas de questions, vous pouvez aussi contacter directement la personne ayant effectué le traitement de données.

Vous avez le droit de :

1. demander une copie des données personnelles que itrust consulting détient sur vous ;
2. demander à itrust consulting de corriger, de mettre à jour, ou de supprimer vos données personnelles dans ses dossiers ; et
3. de signaler toute utilisation abusive de vos données personnelles.

En cas de demande de suppression de vos données, itrust consulting vérifiera qu'il n'y a pas de finalité autre ou de droits d'une autre personne concernée qui l'obligerait à les garder. Dans ce cas, la décision devrait être motivée.

En cas de demande d'une copie de votre dossier, itrust consulting procèdera à une analyse de celui-ci afin d'en supprimer d'éventuelles informations sur d'autres personnes.

Si vous estimez que vos données personnelles n'ont pas été traitées conformément à la loi, vous avez le droit de contacter la CNPD (www.cnpd.lu) ou de déposer une plainte auprès d'elle.

18/06/2024

X 

Carlo Harpes
Gérant
Signed by: Carlo Harpes