

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

1 Informations générales

Dernière mise à jour	20/04/2026
Engagement d'itrust consulting	Le respect de la vie privée de chacun est l'objectif d'itrust consulting, qui s'engage à garantir 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 (ci-après dénommées DCP) et met en œuvre les moyens adéquats pour assurer la protection de vos données et le respect des exigences.
Domaine d'application	La présente déclaration de confidentialité s'applique à toutes les données à caractère personnel transmises à itrust consulting ainsi qu'aux données à caractère personnel que itrust consulting traite dans le cadre de ses activités. Elle ne couvre pas les données relatives aux employés.
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 désigné un délégué à la protection des données (DPO) pour vous aider à exercer vos droits.
Contact DPO	Lynn Pinto dpo@itrust.lu
Modification	itrust consulting se réserve le droit de modifier la présente déclaration de confidentialité en publiant une version mise à jour sur notre site web.

2 Principes d'itrust consulting

itrust consulting accorde une grande importance à la protection des données à caractère personnel. Cela se traduit par la mise en œuvre d'une politique de protection des données propre à itrust consulting.

L'approche d'itrust consulting est basée sur six principes :

1. itrust consulting utilise toujours vos données à caractère personnel de manière équitable et digne de confiance.
2. Elle s'engage à prendre toutes les mesures techniques et organisationnelles appropriées pour garantir la sécurité de vos données à caractère personnel, et en particulier leur confidentialité, leur intégrité et leur disponibilité.
3. Vous avez le droit d'être informé de la manière dont vos données à caractère personnel sont utilisées. itrust consulting fera preuve de transparence à votre égard concernant les données collectées et leur utilisation.
4. Si vous avez des incertitudes quant au traitement de vos données à caractère personnel, veuillez nous contacter afin que nous puissions répondre à vos questions dans les meilleurs délais.
5. Toutes les mesures nécessaires sont prises pour protéger vos informations contre les abus et pour les conserver en toute sécurité.
6. itrust consulting coopère avec la Commission nationale pour la protection des données (ci-après, la CNPD), dont le siège social est situé 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 exclusivement dans le cadre de la mission d'itrust consulting, société spécialisée dans les systèmes de sécurité de l'information, qui aide ses clients des secteurs public et privé à protéger leurs informations contre toute divulgation, manipulation ou indisponibilité. Cette mission consiste à proposer des services liés à :

- la conception, la mise en œuvre et l'audit de systèmes de gestion de la sécurité de l'information,
- l'évaluation et la gestion des risques à l'aide de son propre outil TRICK Service,
- le déploiement d'experts en sécurité en cas de besoin (SECaaS, ou « Security as a Service »),
- le piratage sur demande de nos clients et la gestion des incidents de cybersécurité (malware.lu CERT), ou encore
- la conception et l'exploitation de solutions de sécurité pour les 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 sont limités aux finalités suivantes :

- Gérer les données conformément au contrat (conseil, audit, formation, recherche, etc.).
- Attribuer des identifiants ou des pseudonymes aux élèves passant des tests standardisés ; fournir l'accès au lien à l'enseignant supervisant le test et donnant un retour aux élèves.

- Convertir des ensembles de noms d'élèves présentant des caractéristiques similaires en classes de pseudonymes afin d'effectuer une corrélation statistique entre les résultats des tests et ces caractéristiques, sans révéler l'identité des participants aux tests.
- Proposer des services généraux et sur mesure, recruter des 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.
- Optimiser l'informatique.
- 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 consulting.
- Enquêter sur les manipulations.
- Évaluer l'adéquation des candidats à un poste chez itrust consulting.
- Recueillir des informations sur les candidats sur Internet et auprès de partenaires sous accord de confidentialité (NDA), sauf si le candidat s'y oppose, et recueillir des informations auprès des personnes de référence indiquées par le candidat.
- Conserver la candidature pour réutilisation à d'autres postes jusqu'à ce qu'elle soit clôturée par le candidat.
- Assister les clients dans le cadre d'analyses forensiques et des activités de l'équipe d'intervention en cas d'incident.
- Héberger une base de données de logiciels malveillants, des outils de test de logiciels malveillants et gérer les connaissances techniques liées aux logiciels malveillants.
- Traiter les signalements d'irrégularités conformément à la loi, dans l'intérêt des lanceurs d'alerte (en préservant leur anonymat s'ils le demandent) et du responsable du traitement (en garantissant un retour d'information, une analyse et une correction des problèmes en temps opportun).
- Envoyer les rapports de la plateforme au client concerné et les commentaires du client au lanceur d'alerte

3.3 Qui est concerné par le traitement de données ?

Sont concernés :

- tous les clients, en particulier le personnel des clients en relation avec itrust consulting ;
- tous les partenaires contractuels et sous-traitants ;
- les étudiants et les enseignants concernés par la gestion d'ÉpStan ;
- tous les candidats à un recrutement chez itrust consulting.

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

En ce qui concerne les personnes mentionnées au point 3.3, les données sont collectées auprès de

1. les informations que vous nous communiquez directement ;

2. les informations que nous pouvons recueillir lors de votre navigation sur nos sites web itrust.lu et malware.lu, ainsi que celles provenant de sources telles que LinkedIn, Twitter, etc. ;
3. la base de données gérée par ÉpStan.
4. Internet, des partenaires liés par un accord de confidentialité (NDA) et d'autres personnes sur la base d'un consentement (dans le cadre de l'évaluation des candidats).

Nous n'utilisons pas de processus décisionnels automatisés, y compris le profilage, au sens des lois applicables en matière de protection des données.

Dans le cadre de notre processus de recrutement, nous pouvons consulter des informations vous concernant accessibles au public sur des plateformes de réseautage professionnel (telles que LinkedIn) afin d'évaluer votre candidature.

3.5 De quelles données à caractère personnel dispose itrust consulting ?

Le terme « données à caractère personnel » désigne les informations qui vous identifient ou permettent de vous identifier. Il peut s'agir notamment :

- votre nom, votre adresse, vos identifiants, votre photo de profil, votre adresse e-mail et votre numéro de téléphone ;
- des informations électroniques (adresse IP, données de navigation) ;
- d'autres informations concernant vos activités professionnelles passées ou actuelles, ainsi que les informations, y compris les données à caractère personnel, que vous pourriez nous transmettre ;
- les évaluations des candidats et des employés ;

3.6 Quelle est la base légale du traitement ?

Nous traitons les données à caractère personnel uniquement lorsque nous disposons d'une base juridique valable pour le faire, conformément à la législation applicable en matière de protection des données.

Selon le contexte, nous nous appuyons sur une ou plusieurs des bases juridiques suivantes :

Exécution d'un contrat

Nous traitons les données à caractère personnel lorsque c'est nécessaire pour exécuter un contrat conclu avec vous ou pour prendre des mesures à votre demande avant la conclusion d'un contrat.

Cela comprend, par exemple, la gestion de notre relation avec vous, la fourniture de nos services, ainsi que la gestion de la facturation et des tâches administratives.

Nous traitons les données à caractère personnel pour le compte de notre client B2B conformément aux règles établies dans un contrat et sous la supervision stricte du client, qui agit en tant que responsable du traitement de ces données.

Obligation légale

Nous traitons les données à caractère personnel lorsque cela est nécessaire pour nous conformer aux obligations légales ou réglementaires auxquelles nous sommes soumis. Cela inclut, par exemple, les obligations en matière de comptabilité, de fiscalité et de déclaration.

Intérêts légitimes

Nous traitons les données à caractère personnel lorsque cela est nécessaire pour la poursuite d'intérêts légitimes, à condition que vos droits et libertés fondamentaux ne prévalent pas sur ces intérêts. Nos intérêts légitimes peuvent inclure :

- gérer et améliorer nos services,
- garantir la sécurité de nos systèmes et, par conséquent, protéger nos collaborateurs en cas d'attaque,
- des fins administratives internes,
- prévenir la fraude ou les abus.

Consentement

Nous traitons parfois des données à caractère personnel sur la base de votre consentement, par exemple lorsque les visiteurs du site web acceptent les cookies, ou lorsque nous communiquons les données à caractère personnel de consultants à des clients potentiels afin qu'ils puissent évaluer leurs compétences et leur fiabilité.

Vous avez le droit de retirer votre consentement à tout moment, sans que cela n'affecte la licéité du traitement fondé sur le consentement avant son retrait.

3.7 Quelle est la durée de conservation des données ?

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

Ces durées peuvent toutefois être prolongées en raison de l'application des délais de prescription légaux. Les durées de conservation ont été définies dans le registre des activités de traitement et peuvent être consultées dans les locaux d'itrust consulting. Vous pouvez également consulter le tableau 1 : Durées de conservation issues du registre des activités de traitement, qui présente un résumé du registre. Les données des clients sont conservées pendant toute la durée de la prestation de services avec itrust consulting. Pour toute question concernant la durée de conservation de vos données à caractère personnel, vous pouvez contacter notre délégué à la protection des données.

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

Sous forme anonymisée, les données à caractère personnel peuvent être utilisées à des fins statistiques au-delà de la durée de conservation susmentionnée.

La gestion des connaissances pour la fourniture de services aux entreprises et la gestion des données des clients dans le registre ou le traitement s'effectuent comme suit :

Type de données	Temps de rétention	Délai de suppression après la demande
Conserver les données à caractère personnel à titre de preuve dans le cadre d'une mission de conseil ou d'audit.	10 ans après la fin de l'exercice, sauf en cas de litige en cours devant un tribunal civil : 30 ans (devant un tribunal de commerce : 10 ans) après la fin de l'exercice au cours duquel la décision judiciaire définitive a été rendue.	2 mois
Documents papier relatifs au client.	3 ans après la fin du projet.	2 mois

Rapports de connexion et d'activité (concernant les activités du personnel du client, par exemple les modifications apportées à Owncloud, les connexions à app.trickservice, les conférences MS Teams...)	10 ans (Il s'agit d'une durée maximale ; selon les systèmes, les journaux sont supprimés plus rapidement ou, en cas de mises à jour, par exemple dans MS Teams, ils sont supprimés conformément aux politiques de Microsoft.)	2 mois
Journaux informatiques	5 ans (au maximum)	2 mois
Certains rapports 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 lié à un logiciel malveillant examiné au Parlement luxembourgeois, la première analyse 27001 Gab dans le secteur public...)	30 ans	2 mois
Candidat	2 ans après la clôture par le candidat	2 mois

Table 1: Durée de conservation des registres des activités de traitement pour la gestion des données clients

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

En règle générale, les données à caractère personnel ne sont pas communiquées en dehors d'itrust consulting. L'accès à vos données ne sera accordé qu'aux personnes travaillant chez itrust consulting qui en ont besoin pour l'exercice de leurs fonctions.

Vos données peuvent être traitées par des sous-traitants agissant pour notre compte, notamment :

- notre cabinet comptable (services comptables),
- nos hébergeurs.

Ces prestataires de services sont établis au sein de l'Union européenne et sont soumis à des obligations de confidentialité et de sécurité conformément à la réglementation en vigueur.

Dans le cadre d'enquêtes menées par d'autres autorités (par exemple, une enquête policière), itrust consulting peut être tenue de leur fournir les informations nécessaires à leur enquête.

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

Si nous traitons vos données, vous pouvez envoyer un e-mail au délégué à la protection des données pour en savoir plus sur notre liste de sous-traitants.

3.9 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 transmise à des organisations en dehors de l'UE.

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

L'accès à vos données à caractère personnel est restreint afin d'empêcher tout accès non autorisé, toute modification ou toute utilisation abusive. L'accès n'est accordé qu'aux membres du personnel qui en ont besoin dans le cadre de l'exercice de leurs fonctions.

3.11 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, un PC, un ordinateur portable ou un smartphone) lorsque vous visitez notre site web.

itrust consulting utilise différents types de cookies. Des cookies de session ou de préférences, qui sont indispensables à la navigation et au bon fonctionnement du site. Des cookies d'audience permettant de suivre les informations suivantes concernant les visiteurs. Ces cookies ont pour but de mesurer le nombre d'utilisateurs des services. Des cookies à des fins statistiques permettant de suivre la manière dont les utilisateurs naviguent sur notre site. itrust utilise la solution Matomo, configurée conformément aux recommandations du CEPD afin de se conformer au RGPD. Ces cookies ne contiennent aucune donnée à caractère personnel.

itrust consulting conserve les données collectées par les cookies en les stockant sur les serveurs de données appartenant à itrust consulting et situés au siège social de itrust consulting. Les données sont stockées en Europe.

Les cookies installés par notre site web ne peuvent être lus que par celui-ci. itrust consulting n'utilise pas de service externe pour analyser la manière dont les utilisateurs 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 visant à améliorer la qualité. Vous pouvez accepter ou refuser nos cookies (uniquement les cookies statistiques). Une option par défaut « aucun consentement » s'applique si vous n'avez pas fait de choix. 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 situé dans le coin inférieur droit de notre site web pour « Modifier les paramètres des cookies ».

3.12 Quels sont vos droits et comment les exercer ?

Les dispositions légales relatives à la protection des données à caractère personnel, et notamment les droits des personnes concernées par les opérations de traitement effectuées, s'appliquent dans les conditions prévues et sous réserve des exceptions et dérogations prévues.

Pour toute question relative au traitement de vos données ou pour exercer vos droits, vous pouvez contacter le délégué à la protection des données d'itrust consulting,

- en envoyant un e-mail à l'adresse suivante : dpo@itrust.lu.
- ou par lettre recommandée à l'adresse suivante

itrust consulting s.à r.l.
Délégué à la Protection des Données
55, rue Gabriel Lippmann
L-6947 Niederanven, LUXEMBOURG

en joignant à votre demande une copie lisible et valide de votre pièce d'identité et, le cas échéant, celle de la personne dont vous êtes le représentant légal.

Si vous avez des questions, vous pouvez également contacter directement la personne qui a effectué le traitement des données.

Vous avez le droit de :

1. demander une copie des données à caractère personnel que itrust consulting détient à votre sujet ;
2. demander à itrust consulting de corriger, mettre à jour ou supprimer vos données à caractère personnel de ses fichiers, et
3. signaler toute utilisation abusive de vos données à caractère personnel.

En cas de demande de suppression de vos données, itrust consulting vérifiera qu'aucune autre finalité ou aucun droit d'une autre personne concernée ne l'oblige à les conserver. Dans ce cas, la décision vous sera notifiée.

Si vous demandez une copie de votre dossier, itrust consulting l'analysera afin de supprimer toute information concernant d'autres personnes avant de vous transmettre ce dossier.

Si vous estimez que vos données à caractère personnel 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 de celle-ci.



Recoverable Signature



Carlo Harpes

Managing director

Signed by: 3865b00b-8b7d-4959-9e53-e2aad549deca