intusdata

Réglementation sur le traitement de données de commande

1er septembre 2023

Le présent règlement concrétise les obligations des parties contractantes en matière de protection des données, qui découlent de la relation contractuelle d'Intus Data avec le client. Sont notamment déterminantes les dispositions légales : la loi suisse sur la protection des données (LPD) et l'ordonnance relative à la loi sur la protection des données (OLPD). Cette réglementation s'applique à toutes les activités en rapport avec le contrat et au cours desquelles des données personnelles ("données") du client sont traitées par Intus Data.

1 Objet, durée et spécification du traitement de la commande

L'objet et la durée de la mission ainsi que la nature et la finalité du traitement sont définis dans le contrat.

La durée du présent règlement est fonction de la durée du contrat, à moins que les dispositions du présent règlement n'entraînent des obligations allant au-delà.

Intus Data traite les données à caractère personnel du client en tant que sous-traitant dans les cas suivants :

- lors de la migration de données de systèmes externes vers la solution cible conformément à une commande du client. Dans ce cas, les données personnelles ne sont traitées que dans la mesure où le client les prévoit pour la migration dans la solution cible et les livre à Intus Data (p. ex. données personnelles sur les collaborateurs du client) ;
- dans le cadre d'une commande, pour conserver une copie de la base de données du client (ce qui nécessite une commande séparée du client) à des fins de test ou d'assistance. Dans ce cas, les données personnelles qui ont été enregistrées par le client dans la base de données clients sont traitées (p. ex. les données personnelles des collaborateurs du client) ;
- Dans le cadre de l'abonnement Intus Data Cloud (portail fiduciaire), pour lequel Intus Data exploite le logiciel pour le compte du client, des données personnelles sont traitées et enregistrées par le client dans la base de données mise à disposition par Intus Data (p. ex. données personnelles sur les collaborateurs du client).

2 Champ d'application et responsabilité

Intus Data traite les données personnelles pour le compte du client et selon ses instructions. Dans le cadre de ce contrat, le client est responsable du respect des dispositions légales des lois sur la protection des données pour la légalité du traitement des données ("responsable" au sens de l'art. 5 let. j. LPD).

Les instructions sont définies par le contrat. Les instructions du client qui ne sont pas prévues par le contrat sont traitées comme une demande de modification des prestations et sont payantes.

3 Obligations d'Intus Data

Intus Data ne peut traiter les données des personnes concernées que dans le cadre du mandat et des instructions du client, à moins qu'il n'existe un motif justificatif selon l'art. 9, al. 4, LPD. Intus Data informe immédiatement le client si elle estime qu'une instruction enfreint les lois applicables. Intus Data peut suspendre l'application de l'instruction jusqu'à ce qu'elle soit confirmée ou modifiée par le client.

Dans son domaine de responsabilité, Intus Data concevra l'organisation interne de l'entreprise de manière qu'elle réponde aux exigences particulières de la protection des données. Intus Data prendra des mesures techniques et organisationnelles pour assurer une protection adéquate des données du client, qui répondent aux exigences de la LPD (art. 8 LPD). Elles doivent garantir la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services liés au traitement de manière durable.

Dans la mesure où cela a été convenu et moyennant une rémunération séparée, Intus Data aide le client, dans la mesure de ses possibilités, à répondre aux demandes et aux prétentions des personnes concernées conformément au chapitre 4 de la LPD et à respecter les obligations mentionnées aux articles 24 et 25 de la LPD.

Intus Data garantit que les collaborateurs chargés du traitement des données du client et les autres personnes travaillant pour Intus Data n'ont pas le droit de traiter les données en dehors des instructions données. En outre, Intus Data garantit que les personnes autorisées à traiter les données à caractère personnel se sont engagées à respecter la confidentialité ou sont soumises à un devoir de discrétion légal approprié. L'obligation de confidentialité/de secret professionnel subsiste même après la fin du mandat.

Intus Data informe immédiatement le client lorsqu'elle a connaissance d'une violation de la protection des données à caractère personnel du client. Intus Data prend les

mesures nécessaires pour sécuriser les données et atténuer les éventuelles conséquences négatives pour les personnes concernées et se concerte immédiatement avec le client à ce sujet.

Intus Data indique au client l'interlocuteur pour les questions de protection des données qui se posent dans le cadre du contrat.

Intus Data garantit le respect de ses obligations selon les art. 1 ss. OLPD, de mettre en place une procédure de contrôle régulier de l'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité du traitement.

Intus Data rectifie ou supprime les données faisant l'objet du contrat si le client en donne l'ordre et si cela est compris dans le cadre des instructions. Si une suppression conforme à la protection des données ou une limitation correspondante du traitement des données n'est pas possible, Intus Data se charge de la destruction conforme à la protection des données des supports de données et autres matériels sur la base d'un mandat individuel du client ou restitue ces supports de données au client. Ces prestations doivent être rémunérées séparément.

Les données, les supports de données et tout autre matériel doivent être restitués ou effacés à la demande du client à la fin de la commande.

Si une personne concernée fait valoir des droits à l'encontre du client conformément aux dispositions applicables du droit suisse, Intus Data s'engage à assister le client dans la défense de ses droits dans la mesure de ses possibilités. Ces prestations doivent être rémunérées séparément.

4 Obligations du client

Le client doit informer Intus Data immédiatement et complètement s'il constate des erreurs ou des irrégularités dans les résultats de la commande concernant les dispositions relatives à la protection des données.

En cas de recours du client par une personne concernée concernant d'éventuelles prétentions selon les dispositions applicables du droit suisse, le paragraphe 3, alinéa 10 du présent document s'applique par analogie.

Le client indique à Intus Data l'interlocuteur pour les questions de protection des données qui se posent dans le cadre du contrat.

5 Demandes des personnes concernées

Si une personne concernée s'adresse à Intus Data avec des demandes de rectification, d'effacement ou d'information, Intus Data renvoie la personne concernée au client. Intus Data transmettra immédiatement la demande de la personne concernée au client. Intus Data n'est pas responsable si la demande de la personne concernée n'est pas satisfaite par le client, si elle est incorrecte ou si elle n'est pas satisfaite dans le délai imparti.

6 Moyens de preuve

Sur demande, Intus Data prouve au client le respect des obligations fixées dans le présent contrat par des moyens appropriés.

Si, dans un cas particulier, des inspections par le client sont nécessaires, le client doit faire appel à un expert en protection des données reconnu. L'inspection par l'expert en protection des données doit être effectuée pendant les heures de bureau habituelles, en tenant compte d'un délai de préparation raisonnable. Intus Data peut faire dépendre cet examen de la signature d'une déclaration de confidentialité concernant les données d'autres clients et les mesures techniques et organisationnelles mises en place. Si l'auditeur mandaté par le client entretient une relation de concurrence avec Intus Data, cette dernière dispose d'un droit d'opposition à son encontre. Intus Data peut exiger une rémunération pour l'assistance apportée lors de l'exécution d'une inspection.

Si une autorité de contrôle de la protection des données ou une autre autorité de contrôle souveraine du client procède à une inspection, le paragraphe précédent s'applique en principe par analogie. La signature d'un engagement de confidentialité n'est pas nécessaire si cette autorité de contrôle est soumise à un secret professionnel ou légal.

7 Sous-traitants (autres traitants de commandes)

Le recours à des sous-traitants, à l'exception des filiales d'Intus Data, en tant qu'autres responsables du traitement des données de commande n'est autorisé que si le client a donné son accord préalable.

Le traitement des données dans le cadre de l'abonnement au Cloud fourni par Intus Data (par ex. Vertec Cloud Abo) et de ses services Webaccess fait exception à cette règle.

Intus Data collabore avec des sous-traitants dont la liste figure ici :
https://www.intusdata.ch/fr/sous-traitants/

Il y a relation de sous-traitance soumise à autorisation lorsqu'Intus Data confie à d'autres mandataires tout ou partie de la prestation convenue dans le contrat. Intus Data conclura des accords avec ces tiers dans la mesure

nécessaire pour garantir des mesures appropriées de protection des données et de sécurité des informations.

Si Intus Data confie des mandats à des sous-traitants, il incombe à Intus Data de transmettre au sous-traitant ses obligations en matière de protection des données découlant du présent contrat. Intus Data est en droit de remplacer les sous-traitants sans l'accord explicite du client si les nouveaux sous-traitants garantissent un niveau de protection des données équivalent ou supérieur.

8 Obligation d'information, clause de forme écrite, choix du droit applicable

Si les données du client détenues par Intus Data sont menacées par une saisie ou une confiscation, par une procédure d'insolvabilité ou de règlement judiciaire ou par tout autre événement ou mesure pris par des tiers, Intus Data doit en informer le client sans délai. Intus Data informera immédiatement toutes les personnes responsables dans ce contexte que la souveraineté et la propriété des données appartiennent exclusivement au client.

Toute modification ou tout complément apporté au présent règlement et à tous ses éléments - y compris toute garantie éventuelle de la part d'Intus Data - doit faire l'objet d'un accord écrit, qui peut également prendre la forme d'un format électronique (texte), et doit mentionner expressément qu'il s'agit d'une modification ou d'un complément aux présentes conditions. Cela vaut également pour la renonciation à cette exigence de forme.

9 Responsabilité et dommages-intérêts

Le client et Intus Data sont responsables envers les personnes concernées conformément aux dispositions applicables du droit suisse.

Aperçu des mesures techniques et organisationnelles

10 Principes, protection informatique de base

Le système de gestion de la sécurité de l'information d'Intus Data SA accorde une grande importance à la protection de l'infrastructure informatique ainsi qu'à la formation et à la sensibilisation des collaborateurs aux menaces qui pèsent sur la sécurité de l'information.

Une importance accrue est accordée aux thèmes suivants :

Protection de l'infrastructure client. Les ordinateurs de bureau et les ordinateurs portables des collaborateurs représentent une grande menace pour la sécurité de l'information. Intus Data accorde une très grande importance à la protection de cette infrastructure. Les mesures de protection comprennent entre autres : Solution Endpoint Detection & Response (XDR), antivirus, cryptage des disques durs, systèmes de gestion des correctifs, y compris surveillance et rapports automatiques, durcissement des systèmes contre les attaques via des ports inutilement ouverts. Protection des accès par authentification à deux facteurs (DuoSecurity). La protection de l'infrastructure client implique également de sensibiliser les collaborateurs aux risques liés aux logiciels malveillants et à l'ingénierie sociale.

Séparation des réseaux : les réseaux internes d'Intus Data sont séparés des réseaux de services aux clients. Même les services individuels liés aux clients ne sont reliés entre eux que lorsque cela est absolument nécessaire.

L'accès administratif aux ressources du serveur est limité à une petite équipe d'administrateurs informatiques.

Tous les mots de passe existants ne sont disponibles que pour les utilisateurs qui participent au processus correspondant, selon le principe du "besoin de savoir".

Sécurité physique sur les sites d'Intus Data SA. Les bureaux sont fermés à clé en permanence et les locaux internes des serveurs sont surveillés par des caméras, des détecteurs de fumée et des capteurs de température.

Traitement des données clients (données en possession des clients, pas seulement, mais aussi, données personnelles). Dans le cadre d'un processus mensuel établi, les données des clients (par ex. celles issues des demandes d'assistance) sont identifiées et supprimées si elles ne sont plus nécessaires pour une commande et s'il n'y a pas de demande de stockage permanent.

Les mots de passe des systèmes des clients ne sont enregistrés que conformément à une commande séparée du client. L'enregistrement se fait exclusivement dans le Remote Desktop Manager (devolutions) et est supprimé à la fin de la commande.

11 Traitement de données personnelles sur le réseau interne

Dans le cas d'une commande de migration de données ou d'une commande de stockage d'une base de données, le traitement s'effectue sur le réseau interne d'Intus Data (LAN). Alternativement, la migration des données peut être effectuée sur l'infrastructure du client.

L'accès au LAN d'Intus Data est limité aux appareils protégés conformément à la section 10. Les appareils étrangers sont exclus de l'accès au LAN interne par le matériel (pas de "BYOD").

Une fois le mandat terminé, Intus Data efface les données du client.

12 Intus Data Cloud Abo (Portail fiduciaire)

L'abonnement Intus Data Cloud (portail fiduciaire) permet d'exploiter les logiciels d'Intus Data. Les données personnelles qui sont traitées (et si elles le sont) dépendent du cas d'application concret du client. En règle générale, Intus Data traite les données personnelles du client de manière entièrement automatique, sans traitement manuel ni de modification.

Les exceptions sont les suivantes :

- Contrôle du fonctionnement du système de sauvegarde de la base de données par une restauration aléatoire.
- En cas d'ordre du client de livrer la base de données ou d'ordre du client de restaurer la base de données.
- Dans le cas d'une reprise après sinistre.

L'infrastructure d'abonnement cloud / SaaS est composé de plusieurs serveurs Linux et Windows reliés entre eux et situés en Suisse. L'accès administratif à ces serveurs est fortement limité du point de vue du nombre de personnes. La communication entre les serveurs, entre l'infrastructure d'abonnement au cloud et les applications client ainsi que l'accès administratif est cryptée.