POLITIQUE DE PROTECTION DES DONNEES

thinkproject

ISMS

Système de Management : ISMS
Produits : TOUS
ID du Document : ISMS_00022
Version : 2.0
Classification : Ouverte

Créé par	Andreas Blücher	02.08.2022
Approuvé par	Tom Harman	02.08.2022
Date d'émission originale	03.08.2020	

Veuillez ne pas imprimer de copie de ce document.

TABLE DES MATIÈRES

1 OBJECTIF

Thinkproject est un collectif de produits et de professionnels leaders sur le marché dont l'objectif est de développer et de fournir les meilleures solutions pour soutenir, connecter et faire progresser l'industrie de la construction et les personnes qui la composent.

Cela inclut le traitement des informations et des données pour le compte de nos clients. Par conséquent, les informations des clients doivent être protégées en termes de confidentialité et d'intégrité. La présente politique de protection des données décrit la manière d'atteindre cet objectif et de se conformer aux exigences légales ; notamment le GDPR (règlement général sur la protection des données).

En outre, il peut y avoir des obligations contractuelles qui doivent être prises en compte, par exemple des lieux spécifiques pour le stockage/traitement des données.

Le GDPR contient des clauses d'ouverture pour permettre une réglementation spécifique à chaque pays. Pour se conformer aux extensions nationales du GDPR, il serait pertinent d'obtenir les conseils de consultants locaux lors de la mise en œuvre de politiques régionales de protection des données.

2 DOMAINE D'APPLICATION

Le champ d'application s'applique à l'ensemble du groupe de sociétés TP Holding GmbH qui traite des données personnelles dans l'Union Européenne.

3 DÉFINITIONS ET ABRÉVIATIONS

3.1 Données Personnelles

En général, les données personnelles sont toute information qui se rapporte à une personne physique identifiée ou identifiable. Il peut s'agir par exemple de :

- Nom
- Adresse postale
- Adresse électronique
- Adresse IP
- Données biométriques

3.2 Traitement des Données Personnelles

En termes de GDPR, le traitement des données personnelles signifie : toute opération effectuée sur les données personnelles.

3.3 Licéité du Traitement

Conformément à l'article 6 du GDPR, le traitement n'est licite que si l'une des conditions suivantes s'applique :

1. La personne concernée a donné son consentement
2. Le traitement est nécessaire à l'exécution d'un contrat
3. Le traitement est nécessaire pour le respect d'obligations légales
4. Le traitement est nécessaire pour protéger l'intérêt vital de la personne concernée.
5. Le traitement est nécessaire à l'exécution d'une mission d'intérêt public.
6. Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers.

Dans la plupart des cas, nous nous référerons aux points 1, 2 et 6 dans l'ensemble de notre groupe de sociétés lorsque nous examinerons la relation avec nos clients. En cas de taxes ou de laxisme en matière d'emploi, nous nous référerons au point 3.

3.4 Mesures Techniques et Organisationnelles

Les mesures techniques et organisationnelles sont les fonctions, processus, contrôles, systèmes, politiques, procédures et mesures prises pour protéger et sécuriser les informations personnelles traitées par une organisation.

3.5 Accord sur le Traitement des Données

Un accord de traitement des données est un contrat juridiquement contraignant qui énonce les droits et obligations de chaque partie concernant la protection des données à caractère personnel.

4 RESPONSABILITÉS

4.1 Délégué à la Protection des Données (la terminologie peut varier d'un pays à l'autre)

Les conditions dans lesquelles les entreprises sont tenues de désigner un délégué à la protection des données sont régies par la législation nationale. Il est conseillé aux entreprises de demander conseil sur cette question à un avocat spécialisé dans le droit de la protection des données.

Le délégué à la protection des données (DPD) compétent est chargé de se conformer aux lois et règlements en matière de traitement des données. Ses fonctions sont les suivantes :

- Garantir que les processus et les produits sont conformes au GDPR et aux réglementations spécifiques au pays.
- Tenir des registres locaux des activités de traitement (article 30 du GDPR).
- Interragir avec les autorités de protection des données.
- Interragir avec les clients en matière de protection des données.

Les petites filiales sont autorisées à embaucher des responsables externes de la protection des données après consultation de leur directeur régional.

4.2 Employés

Chaque employé peut entrer en contact avec les données personnelles de nos clients. **Chaque employé est donc tenu de préserver la confidentialité et l'intégrité de ces données et d'agir conformément à la loi. Pour cela, les employés doivent signer un accord de protection des données (on le trouve généralement dans un contrat de travail ou une annexe) et participer à une formation sur la protection des données.**

D'autre part, l'employeur traite les données personnelles des employés. En cas de questions concernant ces traitements, l'employé doit contacter le délégué à la protection des données.

4.3 Responsable de la Sécurité de l'Information

Le responsable de la sécurité de l'information (RSI) veille au respect de cette politique. Il aide le délégué à la protection des données à maintenir la confidentialité et l'intégrité des données.

Le responsable de la sécurité de l'information et le délégué à la protection des données sont tous deux chargés de garantir la confidentialité et l'intégrité des données à caractère personnel, et il peut arriver que les personnes qui assument ces deux rôles doivent travailler ensemble pour atteindre un résultat mutuellement souhaité.

En outre, le responsable de la sécurité de l'information doit s'occuper de la disponibilité. Les mesures visant à accroître la disponibilité des données peuvent avoir une influence négative sur la confidentialité des données. En cas de contradictions, le DPD et le responsable de la sécurité de l'information s'accordent pour parvenir à une protection optimale des données des clients et à la conformité juridique.

4.4 Contrôleur

En ce qui concerne les données des clients, nos clients sont responsables du traitement lorsque nous traitons des données personnelles en leur nom.

En ce qui concerne les employés ou les données collectées sur les sites web des entreprises, nous sommes responsables du traitement de leurs données.

4.5 Sous-traitant

En termes de protection des données, nous sommes appelés le sous-traitant lorsque nous traitons des données personnelles pour le compte de nos clients.

5 EXIGENCES

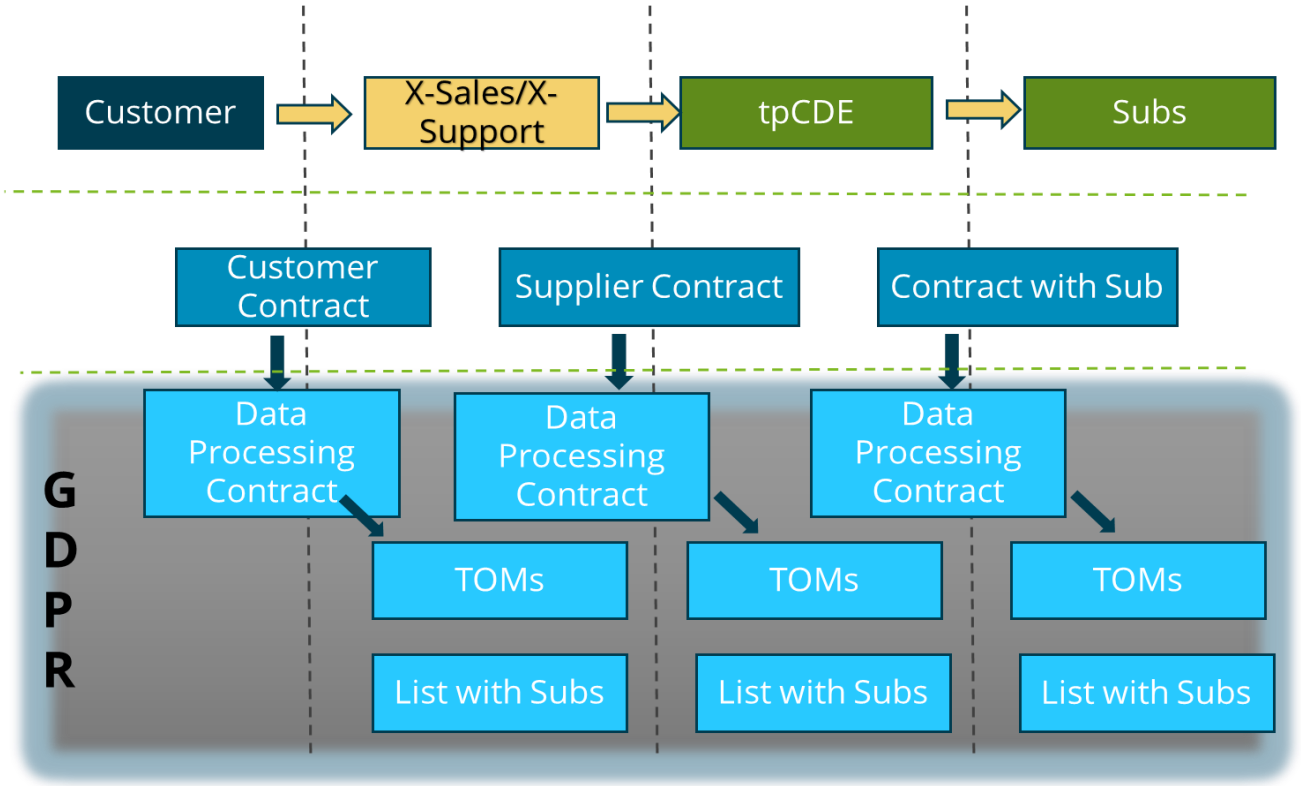
5.1 Principes Relatifs au Traitement des Données à Caractère Personnel

L'article 5 du GDPR énonce six principes relatifs au traitement des données personnelles :

- La licéité, la loyauté et la transparence.
- Limitation de la finalité
- La minimisation des données
- Exactitude
- Limitation du stockage
- Intégrité et confidentialité

5.2 Exigences en Matière de Protection des Données Relatives à nos Clients

Lorsque nous traitons des données personnelles pour le compte de nos clients, nous devons tenir compte des points suivants :



Le client se trouve généralement au début d'une chaîne d'approvisionnement. Il charge l'un de nos bureaux de vente de fournir un service (par exemple un environnement de bureau commun (CDE)). Le service CDE sera fourni par l'un des sites régionaux. Pour fournir ce service, d'autres sous-traitants sont engagés. Lors du traitement des données personnelles dans le cadre du CDE, le GDPR exige que les parties signent un accord de traitement des données (DPA) et fournissent des mesures techniques et organisationnelles (TOM) afin de garantir que le niveau de protection des données reste cohérent tout au long de la chaîne d'approvisionnement.

5.2.1 Accord sur le Traitement des Données (Article 28 du GDPR)

Le traitement par un sous-traitant est régi par un contrat. Ce contrat est connu sous le nom d'accord de traitement des données (APD). Ce contrat doit stipuler que le sous-traitant :

- traite les données à caractère personnel uniquement sur instructions documentées du responsable du traitement
- s'assure que les personnes autorisées à traiter les données à caractère personnel se sont engagées à respecter la confidentialité ou sont soumises à une obligation légale de confidentialité appropriée
- n'engage pas un autre sous-traitant sans l'autorisation écrite spécifique ou générale préalable du responsable du traitement
- maintient le niveau de protection des données au même niveau, même pour les nouveaux sous-traitants
- prévoit des mesures techniques et organisationnelles (TOM) pour assurer la protection des données

- à la demande du responsable du traitement, efface ou renvoie toutes les données à caractère personnel au responsable du traitement après la fin de la prestation des services liés au traitement, et supprime toute copie restante

- met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues par les articles du GDPR, et permet et contribue aux audits, y compris les inspections, réalisés par le responsable du traitement ou un autre auditeur mandaté par le responsable du traitement.

Chaque site qui fournit des logiciels en tant que service et traite les données personnelles des clients doit fournir un modèle d'accord de traitement des données. Ce modèle sera signé à la fois par la société Thinkproject qui traite les données et par le client.

Ce modèle d'accord de traitement des données doit être approuvé par un consultant interne ou externe pour la protection des données.

Parfois, les clients importants fournissent leur propre modèle d'accord de traitement des données. Ce modèle doit être revu au minimum par le responsable de la protection des données et, si nécessaire, par un avocat afin de garantir sa conformité.

5.2.2 Mesures Techniques et Organisationnelles

Selon l'article 32 du RGPD, le responsable du traitement et le sous-traitant des données à caractère personnel doivent mettre en œuvre des mesures techniques et organisationnelles (TOM) appropriées pour assurer un niveau de sécurité des données à caractère personnel.

Ces TOM comprennent la description des mesures visant à assurer :

- le contrôle d'accès (physique)

- le contrôle d'accès (logique)

- le contrôle de la séparation

- le contrôle des relais

- le contrôle des entrées

- le contrôle de disponibilité

- le contrôle des employés

Chaque site qui fournit des logiciels en tant que service et traite les données personnelles des clients doit fournir un modèle de mesures techniques et organisationnelles (TOM). Ces TOMs deviennent une annexe à l'accord de traitement des données.

Les TOM doivent être révisés par un consultant interne/externe pour la protection des données avant d'être partagés avec les clients.

5.2.3 Sous-Traitants

S'il est nécessaire de faire appel à d'autres sous-traitants pour fournir un service à notre/vos client(s) et que ces sous-traitants supplémentaires vont traiter les données personnelles de nos clients, il est nécessaire que les éléments ci-dessous soient en place :

- Un accord de traitement des données signé avec ce sous-traitant.
- Le sous-traitant fournit des mesures techniques et organisationnelles.

5.2.4 Notifications d'une Violation de Données (Article 33 du GDPR)

En cas de violation des données, le responsable du traitement (ici, le client) doit, sans retard excessif et, si possible, au plus tard 72 heures après en avoir pris connaissance, notifier la violation des données personnelles à l'autorité de contrôle (par exemple l'Information Commissioners Office (ICO) au Royaume-Uni), à moins que la violation des données personnelles ne soit pas susceptible d'entraîner un risque pour les droits et libertés des personnes physiques.

Par conséquent, si la violation de données s'est produite au sein d'une partie du groupe Thinkproject lors du traitement des données du client, le client (responsable du traitement) doit être informé à court terme pour pouvoir agir dans les délais fixés. C'est le délégué à la protection des données concerné qui s'en charge. Chaque employé qui constate une violation de données prend immédiatement contact avec le délégué à la protection des données et ouvre un incident ISMS.

Le délai dans lequel le client doit être informé fait souvent l'objet de l'accord de traitement des données (DPA) avec le client. Il est juste de diviser par deux les 72 heures mentionnées ci-dessus dans le DPA, c'est-à-dire 36 heures pour que le sous-traitant notifie le contrôleur et 36 heures pour que le contrôleur notifie l'autorité.

En outre, il faut envisager de consulter un avocat spécialisé dans la protection des données en cas de violation des données afin de minimiser les risques de litiges ou d'amendes imposés par le GDPR (Article 83 du GDPR).

5.2.5 Droits de la Personne Concernée

Conformément au chapitre 3 du GDPR, la personne concernée a les droits suivants :

- Transparence et modalités
- Information et accès aux données personnelles
- Rectification et effacement
- Droit d'opposition et prise de décision automatisée

Les personnes concernées peuvent demander leurs droits au responsable du traitement. Dans le cas où une filiale de Thinkproject est le responsable du traitement des données, les droits doivent être exercés dans un délai d'un mois.

Dans le cas où une filiale de Thinkproject est le sous-traitant, le responsable du traitement (client) doit être impliqué. Il est la personne de contact pour la personne concernée.

5.2.6 Enregistrements des Activités de Traitement

Chaque type d'activité de traitement qui est exécuté en tant que sous-traitant doit être conservé dans un registre des activités de traitement (Article 30 du GDPR).

Ce registre doit contenir toutes les informations suivantes :

1. Le nom et les coordonnées du responsable du traitement
2. La finalité du traitement
3. Une description des catégories de personnes concernées et des catégories de données à caractère personnel.
4. Les catégories de destinataires des données à caractère personnel
5. Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale
6. Si possible, les délais envisagés pour l'effacement des différentes catégories de données
7. Si possible, une description générale des mesures de sécurité techniques et organisationnelles.

Le dossier est tenu par le délégué à la protection des données.

5.3 Exigences en Matière de Protection des Données dans le Développement de Logiciels

Lors du développement de logiciels, les gestionnaires de produits et les développeurs de logiciels doivent tenir compte des points suivants 5.4 et 5.5. :

5.4 Gestionnaires de Produits

- Protection de la vie privée dès la conception (article 25 du GDPR)
- Protection de la vie privée par défaut (article 25 du GDPR)
- Minimisation des données
- Confidentialité et intégrité des données
- Limitation de la finalité
- Limitation du stockage
- Mise en œuvre de fonctionnalités pour les droits des personnes concernées.

5.5 Développeurs de Logiciels

- Protection de la vie privée par défaut (article 25 du GDPR)
- Minimisation des données
- Confidentialité et intégrité des données
- Limitation du stockage

6 SENSIBILISATION DES EMPLOYÉS

6.1 Thinkproject Academy

Chaque employé doit suivre le programme de formation en ligne obligatoire "*GDPR Awareness within Thinkproject*" dans l'Académie Thinkproject. Afin de réussir le cours, les employés doivent répondre à un quiz à la fin du cours. Lorsque les questions sont passées avec un score supérieur à 85%, le participant obtiendra un certificat qui est accessible dans l'Académie Thinkproject. Le certificat est valable un an, les employés sont informés peu avant l'expiration du certificat et sont invités à renouveler leur certification.

Les responsables hiérarchiques reçoivent des rapports bimensuels de l'Académie Thinkproject qui contrôlent le taux de participation de leur équipe. Les responsables hiérarchiques sont chargés de veiller à ce que leurs employés suivent toutes les formations obligatoires. En outre, les taux d'achèvement des employés sont vérifiés chaque année dans le cadre des audits internes.

6.2 Politiques Locales de Protection des Données

Politiques locales de protection des données requises pour la mise en œuvre du GDPR dans ce pays particulier.

7 CONTRÔLES DES DOCUMENTS

Version	Date	Auteur	Approuvé par	Détails des modifications apportées
1.0	22.07.2020	AB	TH	Premier brouillon
1.2	28.07.2020	TH	AB	Révision par TH
1.4	04.08.2020	Alan Brooks	Andreas Blücher	Révision par Alan

1.6	19.11.2020	AB	TH	Droits des personnes concernées
1.0	16.07.2021	KD	AB	Nouvelle numérotation des versions en raison de l'importation dans OneTrust
2.0	21.11.2021	AB	TH	Section TPAcademy avec un lien valide et score de passage correct
2.1	16.05.2022	KD	AB	Ajustement de la section 6.1 (suppression du lien obsolète avec l'environnement de l'académie, changement du titre de la section en sensibilisation).
2.2	02.08.2022	AB	TH	Vérification de la classification, mise en place du statut pour être publié sur le site web