Version: SEP2023

SPECIFICATIONS DE SECURITE TARGIT

Le présent document décrit les mesures de sécurité organisationnelles et techniques mises en œuvre dans le cadre de la fourniture des services par TARGIT et du traitement des données, y compris au travers de TARGIT Cloud, TARGIT Insight et des Services de Support et/ou de Conseil liés à ces services, ou dans le cadre de toute licence on-premise de la solution TARGIT Decision Suite.

1. APPLICABLE À TOUS LES SERVICES

Mesures de sécurité techniques et organisationnelles		
Domaine	**Mesure**	**Description**
Contrôle des accès - Réseau TARGIT	Accès depuis des emplacements externes	L'accès aux systèmes est sécurisé par des procédures d'authentification visant à empêcher tout accès non autorisé aux systèmes et aux applications.
	Gestion des accès	Les processus de gestion des accès garantissent que les droits d'accès sont accordés exclusivement en fonction des besoins professionnels, conformément au principe du moindre privilège. Des procédures sont mises en place pour l'attribution, la suppression et la revue régulière des droits d'accès, sur la base des besoins professionnels et selon le principe de séparation des tâches.
	Gestion des identités et des accès	La gestion des identités et des accès est assurée au moyen de comptes utilisateurs individuels. L'ensemble des comptes est protégé par une authentification multifacteur (MFA) et fait l'objet d'une surveillance des activités suspectes. L'accès aux postes de travail est strictement limité à l'utilisation de noms d'utilisateur et mots de passe individuels.
	Mots de passe	L'ensemble des collaborateurs est tenu de créer des mots de passe sécurisés, conformément à la politique interne de gestion des mots de passe. Les mots de passe sont chiffrés lors de leur stockage. Des règles spécifiques encadrent la création des mots de passe et les utilisateurs sont informés lorsqu'un renouvellement de mot de passe est requis.

	Chiffrement	Les données en transit sont chiffrées à l'aide du chiffrement TLS (SSL). Les partages de fichiers Azure, les comptes de stockage et Cosmos DB sont chiffrés au repos et en transit.
	Pare-feu	Des pare-feu sont installés afin de protéger contre tout accès non autorisé.
	Tests d'intrusion	Des tests d'intrusion sont réalisés de manière annuelle.

	Protection contre les logiciels malveillants	Des logiciels antivirus sont déployés sur l'ensemble des postes informatiques, et tout logiciel téléchargé fait l'objet d'une surveillance afin de détecter les menaces potentielles.
	Anti-spam et anti-hameçonnage	Des solutions anti-spam et anti-hameçonnage sont mises en œuvre sur le système de messagerie interne.
	Politique Clean Desk	L'utilisation de documents physiques est très limitée. Lorsque des documents physiques existent, ils sont systématiquement stockés de manière sécurisée lorsqu'ils ne sont pas utilisés.
	Brute-force attacks	Les comptes utilisateurs sont automatiquement verrouillés après un nombre prédéfini de tentatives de connexion infructueuses liées à des mots de passe incorrects.
Contrôle des accès – Données client	Contrôle par le Client	Seules les personnes désignées par le Client et ayant, conformément aux instructions du Client adressées à TARGIT, reçu des identifiants d'accès au Service fournis par TARGIT, sont autorisées à accéder aux Données Client. En règle générale, les employés de TARGIT n'ont pas accès aux Données Client. Le Client peut octroyer aux employés de TARGIT un identifiant utilisateur (délivré par le Client) afin de permettre à l'employé de TARGIT d'accéder aux Données client. Un nombre limité d'employés de TARGIT disposant de droits d'administrateur sur la solution Cloud peut accéder aux Données Client si cela est nécessaire à l'exploitation et au fonctionnement du système.
	Système d'autorisation	Le Client peut mettre en place un système d'autorisations basé sur des rôles, avec des droits d'accès différenciés, et attribuer ces rôles à des utilisateurs spécifiques.

	Confidentialité et séparation	L'accès de TARGIT aux Données Client est encadré par des engagements contractuels, des déclarations de confidentialité et la mise en œuvre d'une séparation fonctionnelle, afin de réduire le risque d'erreur et d'utilisation abusive des données.
	Chiffrement	Les données en transit sont chiffrées à l'aide du chiffrement TLS (SSL). Les partages de fichiers Azure, les comptes de stockage et Cosmos DB sont chiffrés au repos et en transit.
	Sécurité des connexions	Le Client peut activer l'authentification à deux facteurs (MFA) lors de la connexion au système, notamment lorsqu'il utilise des fournisseurs d'identité OpenID.
	Suppression des Données Client	Les Données Client peuvent être supprimées par le Client ou, à la demande du Client, à tout moment. Toute Donnée Client stockée sera supprimée à la résiliation de l'Abonnement du Client.
Personnel	Comptes des employés	Des procédures et des scripts automatisés garantissent que les comptes des nouveaux employés sont correctement configurés, avec une authentification multifacteur et des niveaux d'accès appropriés.

	Sensibilisation, formation et information	Les employés reçoivent une formation sur les systèmes informatiques et une sensibilisation à la sécurité informatique, au RGPD et aux politiques internes de sécurité et de protection de la vie privée. La participation à ces formations est obligatoire pour tous les employés. TARGIT a mis en place un processus établi garantissant que toute personne intervenant pour le compte de TARGIT et ayant accès aux Données Client a pleinement connaissance de ses responsabilités en matière de sécurité de l'information. TARGIT veille à ce que toute personne physique intervenant pour son compte et ayant accès aux Données Client ne traite ces données que conformément aux instructions documentées du Client, sauf si un autre traitement est requis par la législation applicable.
	Retrait des droits d'accès	Les droits d'accès sont révoqués en cas de cessation de la relation de travail. Des procédures sont en place afin de garantir que les comptes des collaborateurs sont clôturés correctement.

	Accords de confidentialité (NDA)	Les accords de confidentialité (NDA) font partie intégrante des contrats conclus avec les employés, les consultants externes et, le cas échéant, les autres partenaires commerciaux.
Sécurité physique	Procédures de contrôle d'accès	TARGIT empêche tout accès non autorisé aux sites physiques de TARGIT au moyen de procédures de contrôle d'accès appropiées.
	Protection physique	TARGIT a organisé et mis en place des mesures de protection physique de ses sites, notamment contre les catastrophes naturelles, les actes malveillantes ou les accidents.
	Alarmes anti-intrusion	Des système d'alarme sont installées dans tous les locaux afin de prévenir les intrusions, les vols ou les actes de vandalisme.
	Prévention des incendies	Des systèmes de sprinklers anti-incendie sont installés à l'intérieur des locaux.
	Accès à distance	L'accès à distance aux ressources de tout sous-traitant de traitement de données nécessite l'utilisation d'une connexion VPN sécurisée.
Politiques, procédures et organisation de la sécurité	Conformité aux lois et réglementation	Un suivi continu de la législation et des pratiques en vigueur, ainsi que des évolutions réglementaires, est assuré.
	Politique de confidentialité	Tous les employés sont tenus de prendre connaissance et de respecter la politique de confidentialité de TARGIT, laquelle définit les règles applicables au traitement des Données Client, y compris les données à caractère personnel, conformément au RGPD et aux réglementations nationales applicables.
	Procédure de gestion des incidents de sécurité	Une procédure de gestion des incidents de sécurité est en place et doit être connue et appliquée par l'ensemble des employés.
	Politique de sécurité	TARGIT dispose d'une politique interne de sécurité de l'information approuvée par la direction.

		La politique de sécurité est révisée annuellement et mise à jour chaque fois que nécessaire. L'ensemble des activités de traitement est réalisé conformément à des directives internes définissant des exigences spécifiques en matière de sécurité, incluant notamment des règles relatives à l'autorisation, à

		l'administration des accès, au contrôle des accès et à la journalisation des tentatives de connexion.
	Évaluation des risques	TARGIT procède à des évaluations des risques de manière continue, en tenant compte de l'évolution des pratiques et des menaces dans le domaine de la sécurité de l'information, et examine, ajuste et met en œuvre les mesures techniques et organisationnelles nécessaires afin de traiter les risques identifiés.
	Organisation de la sécurité	ARGIT a mis en place au sein de son organisation une répartition clairement définie des rôles et responsabilités afin de garantir la sécurité de l'information.
	Plan de reprise d'activité	Un plan de reprise d'activité est mis en œuvre et testé régulièrement.

2. APPLICABLE UNIQUEMENT À TARGIT INSIGHT POUR LES CLIENTS TARGIT DECISION ON-PREMISE

Les journaux relatifs à l'utilisation des documents dans TARGIT Decision Suite sont stockés dans des fichiers locaux hébergés sur le serveur du Client.

Lors de l'activation de TARGIT Insight, ces fichiers sont transférés vers l'environnement d'hébergement TARGIT Insight sur Microsoft Azure. TARGIT Insight implique alors ce qui suit :

- Une base de données chiffrée, dédiée spécifiquement au Client, est créée sur le serveur Microsoft Azure SQL de TARGIT (la « **Base de données Azure SQL** »).
- Un identifiant SQL et un mot de passe sont générés automatiquement pour l'utilisation de la Base de données Azure SQL et ne sont communiqués ni au Client ni aux employés de TARGIT.
- TARGIT Insight transmet les informations de connexion au serveur du Client. Ces informations ne sont pas stockées localement et sont conservées uniquement en mémoire. Cette connexion est configurée en lecture seule (read-only).
- Les seules données à caractère personnel stockées par TARGIT Insight sont les noms d'utilisateur et les droits d'accès des utilisateurs aux rapports et documents. Le nom d'utilisateur correspond à celui utilisé par un agent ou un employé du Client pour se connecter au client TARGIT.
- Les données issues des fichiers Client transférés sont traitées et stockées dans la Base de données Azure SQL.
- Toutes les communications entre le serveur du Client et la Base de données Azure SQL sont chiffrées via SSL/TLS.
- L'accès à la Base de données Azure SQL est restreint au moyen de groupes de sécurité et seuls les employés de TARGIT impliqués dans le support ou la fourniture de services au Client peuvent y accéder, et uniquement selon le principe du besoin d'en connaître (need-to-know).