Fourniture du vertical EnkiSys pour Microsoft 365 Business Central et réalisation de prestations et services associés

Entité : TBS
Domaine : Clients

Description générale

Nom du traitement	Référence	Envisagé	Archivé
Fourniture du vertical EnkiSys pour Microsoft 365 Business Central et réalisation de prestations et services associés	APPSOURCE_BC_0005	Oui	Non

Date de création	Date de modification	Date de revue
22/11/2024	22/11/2024	22/11/2024

Description
Fourniture du vertical EnkiSys pour Microsoft 365 Business Central et réalisation de prestations et services associés. Le vertical a pour but de fournir des fonctionnalités complémentaires à business Central pour la gestions de chantiers, de matériel et de sous-traitance.

Structure opérationnelle	Volumétrie
Business Central	

Origine de la collecte des données	Description de la source
Collecte indirecte	Récolte des données par Microsoft 365 Business Central.

Supports

Référence	Support
APP11	Microsoft Azure

Politiques

Référence	Politique
PAS	Plan d'assurance sécurité
POL_02	Politique de protection des droit des personnes concernées
BFM_PSSI	Politique de sécurité du système d'information

Acteurs

Type d'acteur	Nom	Adresse	Code postal	Ville	Pays	Coordonnées contact
Référent opérationnel	Vincent Bourassa	2 Rue Jacques Villermaux	54000	Nancy	France	vbourassa@talent-bs.com
Responsable du traitement	Talent Business Solutions	4 Rue Jean Monnet	67201	Eckbolsheim	France	+33 7 88 16 10 21
Délégué à la protection des données	DPO de Talent Business Solutions	4 Rue Jean Monnet	67201	Eckbolsheim	France	+33 7 84 10 23 96

Finalités

Finalité principale	
Description	Fourniture du vertical EnkiSys pour Microsoft 365 Business Central et réalisation de prestations et services associés

Finalités	
Fondement juridique	Exécution d'un contrat ou mesures pré-contractuelles
Commentaire	
Sous-finalité	
Description	Mise en place de la solutions
Fondement juridique	Exécution d'un contrat ou mesures pré-contractuelles
Commentaire	Envoi du package d'installation au client et éventuellement assistance à l'installation
Sous-finalité	
Description	Télésurveillance et statistique d'utilisations
Fondement juridique	Intérêt légitime du responsable de traitement
Commentaire	Télésurveillance et statistique d'utilisations anonymisées du produit sur le tenant des clients
Sous-finalité	
Description	Support et maintenance de la solution
Fondement juridique	Exécution d'un contrat ou mesures pré-contractuelles
Commentaire	Intervention dans le cadre du support et de la maintenance de la solution. Ces action peuvent nécessiter des modifications de données dans le Business Central du client.

Personnes concernées	
Catégorie de personnes concernées	Commentaires
Clients	
Fournisseurs	
Prospects	
Salariés	
Sous-traitants	

Destinataires			
Service interne qui traite les données			
Destinataire	Chef de projet		
Commentaire	Suivi du projet et de la télémétrie		
Service interne qui traite les données			
Destinataire	Consultants et Dévelopeurs BC		
Commentaire	Personnalisation, configuration, maintenance et support du vertical		
Sous-traitants			
Destinataire	Microsoft	Cadre juridique existant	X
Commentaire	Hébergement de la télémétrie.		

Données à caractère personnel	
Etat-civil, identité, données d'identification	
DCP	Nom, prénom, adresse mail du contact chez le client
Destinataire des DCP	Consultants et Dévelopeurs BC, Chef de projet
Finalité	Mise en place de la solutions
Durée de conservation	Durée du contrat
Etat-civil, identité, données d'identification	
DCP	Nom, prénom, téléphone et adresse mail des fournisseur, clients, sous-traitant et salariés
Destinataire des DCP	Consultants et Dévelopeurs BC, Microsoft, Chef de projet
Finalité	Support et maintenance de la solution
Durée de conservation	Pour la duréedu traitement en base active et 5 ans en archivage intermédiaire

Données à caractère personnel

Etat-civil, identité, données d'identification	
DCP	Nom, prénom, téléphone et adresse mail des fournisseur, clients, sous-traitant et salariés
Destinataire des DCP	Consultants et Dévelopeurs BC, Microsoft, Chef de projet
Finalité	Fourniture du vertical EnkiSys pour Microsoft 365 Business Central et réalisation de prestations et services associés
Durée de conservation	Durée du contrat
Etat-civil, identité, données d'identification	
DCP	Nom, prénom, téléphone et adresse mail des fournisseur, clients, sous-traitant et salariés
Destinataire des DCP	
Finalité	Fourniture du vertical EnkiSys pour Microsoft 365 Business Central et réalisation de prestations et services associés
Durée de conservation	A définir
Données de connexion (adresses IP, journaux d'événements...)	
DCP	Données de télémétrie et d'utilisation annonymisées
Destinataire des DCP	Consultants et Dévelopeurs BC, Microsoft, Chef de projet
Finalité	Télésurveillance et statistique d'utilisations
Durée de conservation	3 mois

Opérations

Collecte	
Description détaillée du processus	Collecte de données de télémétrie et d'utilisation pour faciliter support et la maintenance.
Type de support	Applications/Logiciels
Supports sur lesquels reposent les données à caractère personnel	Microsoft Azure,
Autres supports	
Conservation	
Description détaillée du processus	Stockage des données de télémétrie et d'utilisation
Type de support	Applications/Logiciels
Supports sur lesquels reposent les données à caractère personnel	Microsoft Azure,
Autres supports	
Utilisation	
Description détaillée du processus	Statistiques annonymisées des données de télémétrie et d'utilisation
Type de support	Applications/Logiciels
Supports sur lesquels reposent les données à caractère personnel	Microsoft Azure,
Autres supports	

Mesures de nature juridique

Minimisation : réduction des données à celles strictement nécessaires	
Périmètre	Politique de protection des droit des personnes concernées
Description et justification	Seules les données nécessaires sont traitées dans le cadre du traitement
Qualité : préservation de la qualité des données à caractère personnel	
Périmètre	Politique de protection des droit des personnes concernées
Description et justification	Nous vérifions que les données collectées soient de qualités
Information : respect du droit à l'information des personnes concernées	
Périmètre	Politique de protection des droit des personnes concernées
Description et justification	Lors de la collecte directe de données, nous fournissons la politique de confidentialité expliquant le

Mesures de nature juridique	
	traitement. Lors de la collecte indirecte, nous envoyons, et ce, dans un délai d'un mois maximum après réception des données personnelles, la politique de confidentialité.
Droit d'opposition : respect du droit d'opposition des personnes concernées	
Périmètre	Politique de protection des droit des personnes concernées
Description et justification	Conformément au Droit d'opposition, la personne concernée a le droit de s'opposer au traitement de ses données. À la réception de cette demande, le service en charge du traitement cessera le traitement des données de la personne, après avoir vérifié son identité. Cette demande sera examinée et traitée dans un délai maximal d'un mois.
Droit d'accès : respect du droit des personnes concernées d'accéder à leurs données	
Périmètre	Politique de protection des droit des personnes concernées
Description et justification	À la demande de la personne concernée, le service en charge du traitement fournit une copie des données traitées après avoir vérifié l'identité de la personne. Cette demande sera étudiée et traitée dans un délai maximal d'un mois.
Droit de rectification : respect du droit des personnes concernées de corriger leurs données et de les effacer	
Périmètre	Politique de protection des droit des personnes concernées
Description et justification	À la demande de la personne concernée, le service en charge du traitement rectifie les données inexactes ou incomplètes en vérifiant l'identité de la personne. Cette demande sera étudiée et traitée dans un délai maximal d'un mois.
Droit à la portabilité : respect du droit à la portabilité des données à caractère personnel	
Périmètre	Politique de protection des droit des personnes concernées
Description et justification	À la demande de la personne concernée, le service en charge du traitement fournit les données dans un format structuré, couramment utilisé et lisible par machine, ou transfère les données à un autre responsable du traitement, après avoir vérifié l'identité de la personne. Cette demande sera étudiée et traitée dans un délai maximal d'un mois.
Droit à la limitation : respect du droit à la limitation des traitements des données à caractère personnel	
Périmètre	Politique de protection des droit des personnes concernées
Description et justification	À la demande de la personne concernée, le service en charge du traitement limite le traitement des données lorsque les conditions légales sont remplies, après avoir vérifié l'identité de la personne. Cette demande sera étudiée et traitée dans un délai maximal d'un mois.
Droit à l'effacement	
Périmètre	Politique de protection des droit des personnes concernées
Description et justification	À la demande de la personne concernée, le service en charge du traitement supprime les données demandées en vérifiant l'identité de la personne. Cette demande sera étudiée et traitée dans un délai maximal d'un mois.
Droit à ne pas faire l'objet d'une décision entièrement automatisée	
Périmètre	Politique de protection des droit des personnes concernées
Description et justification	En vertu du droit à ne pas faire l'objet d'une décision entièrement automatisée, la personne concernée peut demander une intervention humaine si une décision automatisée a été prise. Le service en charge du traitement examinera la décision, en tenant compte des opinions et des arguments de la personne concernée. Cette demande sera traitée dans un délai maximal d'un mois, après vérification de l'identité de la personne.
Obligation d'assurer la chaîne des droits	
Périmètre	Politique de protection des droit des personnes concernées
Description et justification	Lorsqu'une personne concerné décide d'exercer l'un de ses droits, la demande sera transmise par le service responsable du traitement des données aux entités tierces impliquées dans le traitement.

Mesures organisationnelles	
Politique (gestion des règles)	
Périmètre	Microsoft Azure
Description et justification	Gestion des rôles et permissions

Mesures de sécurité logique	
Anonymisation	
Périmètre	Microsoft Azure
Description et justification	Contrôle strict des accès aux données anonymisées
Chiffrement	
Périmètre	Microsoft Azure
Description et justification	Chiffrement symétrique des données
Chiffrement	
Périmètre	Microsoft Azure
Description et justification	Chiffrement asymétrique des données
Chiffrement	
Périmètre	Microsoft Azure
Description et justification	Mise en place d'algorithmes d'encryptions réputés
Chiffrement	
Périmètre	Microsoft Azure
Description et justification	Utilisation de clés de chiffrement robustes
Chiffrement	
Périmètre	Microsoft Azure
Description et justification	Gestion des cycles de vie des clés de chiffrement
Contrôle d'intégrité	
Périmètre	Microsoft Azure
Description et justification	Utilisation de fonctions de hachage sécurisées
Contrôle d'intégrité	
Périmètre	Microsoft Azure
Description et justification	Utilisation de codes d'authentification de message
Contrôle d'intégrité	
Périmètre	Microsoft Azure
Description et justification	Protection contre les injections SQL et autres attaques
Sauvegardes	
Périmètre	Microsoft Azure
Description et justification	Réplication des sauvegardes sur un autre lieu physique
Sauvegardes	
Périmètre	Microsoft Azure
Description et justification	Planification et exécution régulières de sauvegardes
Sauvegardes	
Périmètre	Microsoft Azure
Description et justification	Chiffrement des sauvegardes
Sauvegardes	
Périmètre	Microsoft Azure
Description et justification	Stockage sécurisé des sauvegardes
Cloisonnement (données, réseau)	
Périmètre	Microsoft Azure
Description et justification	Isolation des données et ressources pour chaque client
Cloisonnement (données, réseau)	
Périmètre	Microsoft Azure
Description et justification	Classification des données
Cloisonnement (données, réseau)	
Périmètre	Microsoft Azure
Description et justification	Séparation logique des données : environnements distincts

Mesures de sécurité logique	
Cloisonnement (données, réseau)	
Périmètre	Microsoft Azure
Description et justification	Audit et surveillance des accès aux données
Cloisonnement (données, réseau)	
Périmètre	Microsoft Azure
Description et justification	Segmentation du réseau
Contrôle d'accès logique	
Périmètre	Microsoft Azure
Description et justification	Mise en place d'une solution d'authentification multi-facteur
Contrôle d'accès logique	
Périmètre	Microsoft Azure
Description et justification	Gestion des rôles et permissions
Contrôle d'accès logique	
Périmètre	Microsoft Azure
Description et justification	Gestion d'une identité utilisateur unique avec le SSO
Contrôle d'accès logique	
Périmètre	Microsoft Azure
Description et justification	Politique de mots de passe robuste
Contrôle d'accès logique	
Périmètre	Microsoft Azure
Description et justification	Principe du moindre privilège
Traçabilité	
Périmètre	Microsoft Azure
Description et justification	Journalisation des événements
Traçabilité	
Périmètre	Microsoft Azure
Description et justification	Cycle de vie des journaux d'événements
Exploitation	
Périmètre	Microsoft Azure
Description et justification	Documentation des procédures d'exploitation
Exploitation	
Périmètre	Microsoft Azure
Description et justification	Correction des vulnérabilités
Exploitation	
Périmètre	Microsoft Azure
Description et justification	Réplication des données
Exploitation	
Périmètre	Microsoft Azure
Description et justification	Inventaire complet des logiciels et matériels utilisés
Surveillance (paramétrages, contrôles de configurations, surveillance en temps réel...)	
Périmètre	Microsoft Azure
Description et justification	Configuration des outils de surveillance
Surveillance (paramétrages, contrôles de configurations, surveillance en temps réel...)	
Périmètre	Microsoft Azure
Description et justification	Journalisation détaillée
Surveillance (paramétrages, contrôles de configurations, surveillance en temps réel...)	
Périmètre	Microsoft Azure

Mesures de sécurité logique

Description et justification	Respect des obligations en matière de protection des données
Lutte contre les codes malveillants (virus, logiciels espions, bombes logicielles...)	
Périmètre	Microsoft Azure
Description et justification	Utilisation d'anvirus et d'anti-malware
Lutte contre les codes malveillants (virus, logiciels espions, bombes logicielles...)	
Périmètre	Microsoft Azure
Description et justification	Sensibilisation et formation des utilisateurs
Lutte contre les codes malveillants (virus, logiciels espions, bombes logicielles...)	
Périmètre	Microsoft Azure
Description et justification	Remontée des événements de sécurité
Protection des canaux informatiques (réseaux)	
Périmètre	Microsoft Azure
Description et justification	Utilisation de protocoles de communication sécurisés
Protection des canaux informatiques (réseaux)	
Périmètre	Microsoft Azure
Description et justification	Mise en place d'une défense en couche
Protection des canaux informatiques (réseaux)	
Périmètre	Microsoft Azure
Description et justification	Cartographie complète du réseau
Protection des canaux informatiques (réseaux)	
Périmètre	Microsoft Azure
Description et justification	Mise en place d'un système de détection et prévention d'intrusion (IDS/IPS)

Transferts vers des pays tiers

Microsoft	
Pays	France
Conformité	Union Européenne
Type de garantie	Décision d'adéquation
Justification	

Facteurs de risque

Facteurs de risque	
Sensibilité	
Traitement sensible :	
Traitement exonéré :	
Justification :	