COSMO CONSULT
Business-Software für Menschen

PROTECTION ET SECURITE DES DONNEES CHEZ COSMO CONSULT

Version : 3.2 | 13.09.2019

1 TABLE DES MATIÈRES

Protection et sécurité des données chez COSMO CONSULT

1. Mesures générales de protection des données chez COSMO CONSULT

Lorsque les données sont traitées pour le compte du responsable du traitement, le sous-traitant n'est pas une tierce partie aux termes de la réglementation relative à la protection des données ; le responsable du traitement demeure responsable de la protection des données en vertu de la réglementation externe en matière de protection des données.
Par conséquent, le responsable du traitement est tenu de vérifier par lui-même que le sous-traitant met en œuvre les mesures techniques et organisationnelles adéquates et nécessaires à ce type de traitement.
La présente Annexe décrit les mesures techniques et organisationnelles que le sous-traitant associé à l'externalisation doit mettre en œuvre conformément à l'Article 32 du RGPD.
Elle décrit les mesures concrètes utilisées en vue de protéger les données traitées des abus éventuels au regard de la finalité de la protection et du type de données.

1.1 COSMO CONSULT a adopté les mesures nécessaires pour garantir la sécurité des objets et données ainsi que la continuité des activités du site en termes de construction, de personnel, d'organisation et de technologie.

1.2 COSMO CONSULT est tenu au secret professionnel envers ses clients. L'ensemble des employés de COSMO CONSULT se sont engagés à respecter la confidentialité des données lors de leur recrutement.

1.3 Chez COSMO CONSULT, le périmètre de protection englobe la manipulation des données des personnes physiques ou morales ainsi que la manipulation des autres données confidentielles ou sensibles (données financières ou d'entreprise, par exemple).

1.4 COSMO CONSULT a déployé des mesures de lutte contre les incendies et les pertes dans l'ensemble de ses sites et bureaux.

1.5 Dans l'ensemble des sites, les dispositions de contrôle des accès et sorties sont mises en œuvre par un système de sécurité structurelle pour les bureaux et, en règle générale, par des zones de surveillance électronique. L'élimination des documents confidentiels est assurée exclusivement par un système de destruction ou des déchiqueteuses.

1.6 COSMO CONSULT utilise les technologies Microsoft nouvelle génération qui répondent à l'ensemble des dispositions en matière de protection des données. En témoignent les nombreux labels de protection des données dont bénéficient les produits Microsoft.

1.7 COSMO CONSULT emploie plusieurs spécialistes informatiques certifiés (généralement Microsoft) pour vérifier les précautions de sécurité mises en œuvre, les étendre conformément aux dispositions applicables et les développer au regard des nouvelles mesures de sécurité.

1.8 COSMO CONSULT traite les données dans le cadre du déploiement logiciel à des fins de migration et d'essai. Par ailleurs, COSMO CONSULT configure ses systèmes d'essai en collaboration avec le client. Les systèmes d'essai sont conservés pendant toute la durée du support de COSMO CONSULT ou pendant la durée convenue au contrat. Après consultation du client, les jeux de données des systèmes d'essai peuvent constituer des ensembles qui ont été adaptés aux données sensibles et simulés à des fins d'essai.

1.9 Un dispositif de sécurité (chiffrement, etc.) prévient systématiquement les accès non autorisés en cas de maintenance et d'accès à distance aux systèmes du client.

1.10 Afin de prévenir tout virus informatique, l'ensemble des supports, messages électroniques et pièces jointes entrants sont soumis à des analyses antivirus. Par ailleurs, l'ensemble des ordinateurs et serveurs sont protégés par un système Endpoint Protection centralisé.

1.11 COSMO CONSULT a migré la quasi-intégralité de ses services centralisés et dispositions de protection des données vers un datacenter central.

1.12 Le traitement de données s'effectue exclusivement dans le cadre du RGPD de l'UE.

1.13 Si un accord de traitement externalisé a été conclu avec le client, les mesures complémentaires de protection des données suivantes s'appliquent :

1.13.1 Le principe de séparation des fonctions existe pour toutes les sphères stratégiques. Les sphères visées par le traitement de données sont dissociées sur le plan fonctionnel et organisationnel. Les systèmes clients sont uniquement accessibles aux employés autorisés, ainsi qu'à l'équipe de projet et de support client dédiée. Les droits d'accès sont attribués par le chef de projet concerné et régulièrement vérifiés.

1.13.2 Les données d'accès par réseau commuté nécessaires à la maintenance à distance sont personnalisées ou uniquement accessibles aux employés autorisés de l'équipe de projet ou de support client dédiée, en fonction des dispositions du client.

1.13.3 COSMO CONSULT prend la protection et la sécurité des données très au sérieux. C'est pourquoi COSMO CONSULT fait régulièrement auditer ses processus internes.

2. Mesures techniques et organisationnelles

2.1 Les mesures techniques et organisationnelles concernent les activités suivantes :

2.1.1 Contrôle des externalisations, contrôle d'accès physique, contrôle d'accès logique, contrôle d'accès aux données, contrôle de transmission des données, contrôle des entrées, contrôle de la disponibilité, contrôle de la séparation et contrôle de l'efficacité.

2.1.2 Type d'échange de données, fourniture des données, types et conditions de traitement, conservation des données, types et conditions de transmission des données.

2.1.3 Mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résistance des systèmes et services de manière continue ; capacité à rétablir rapidement l'accessibilité et la disponibilité des données à caractère personnel en cas d'incident physique ou technique.

2.1.4 Procédure de réexamen périodique, d'évaluation et de validation de l'efficacité de ces mesures.

2.2 Dans la mesure où les services sont hébergés par un sous-traitant ultérieur, COSMO CONSULT devra sélectionner ces derniers exclusivement sur la base des dispositions légales, les engager par écrit et informer les clients du contrat à conclure en matière de traitement de données externalisé.

2.3 Le groupe COSMO CONSULT vérifie et valide régulièrement la conformité aux mesures techniques et organisationnelles adoptées par l'ensemble des entreprises liées par l'Accord de contrôle conjoint conformément aux modalités de l'Article 26 du RGPD.

2.4 En général, les mesures techniques et organisationnelles de COSMO CONSULT reposent sur des progrès techniques et d'autres innovations. COSMO CONSULT s'engage à mettre en œuvre l'ensemble des mesures nécessaires pour renforcer la sécurité.
La documentation récente des mesures techniques et organisationnelles intitulée « Protection et sécurité des données chez COSMO CONSULT » est disponible en téléchargement sur le site web : https://www.cosmoconsult.com/data-protection.

2.5 Sites de traitement de données

2.5.1 Datacenter central de COSMO CONSULT

COSMO CONSULT héberge l'intégralité de ses services et serveurs centralisés sur Microsoft Azure.

Pour plus d'informations, rendez-vous sur https://azure.microsoft.com.

2.5.2 Sites COSMO CONSULT

COSMO CONSULT est un groupe international d'entreprises dont les différents sites sont chargés d'exécuter des projets informatiques dans le monde entier. Les réglementations et mesures documentées dans les présentes s'appliquent à l'ensemble des sites du groupe COSMO CONSULT visés par l'Accord de contrôle conjoint.

Pour plus d'informations, rendez-vous sur : https://www.cosmoconsult.com/data-protection

2.5.3 Traitement de données via Microsoft Azure

Si le client opte pour l'hébergement de ses données sur une plateforme Azure et que le transfert des données à caractère personnel en dehors de l'Europe ne peut être exclu, un contrat a été signé avec Microsoft Ireland Operations Limited, Atrium Building Block B, Carmenhall Road, Sandyford Industrial Estate, Dublin 18, Irlande conformément aux dispositions légales. L'adéquation du niveau de protection des données est par ailleurs garantie par une certification valide en vertu du Privacy Shield.

Pour en savoir plus :

https://www.privacyshield.gov/pmodalityicipant?id=a2zt0000000KzNaAAK&contact=true#dispute-resolution-1

2.6 Contrôle d'accès physique

Les paragraphes suivants décrivent les mesures destinées à prévenir toute intrusion forcée ou non autorisée au sein des bureaux de COSMO CONSULT.

La sécurité des salles de serveurs locales (le cas échéant) a été renforcée dans l'ensemble des bâtiments de bureaux.

2.6.1 Mesures techniques

Modalité	Applicabilité
Contrôle d'accès physique	Oui
Système de verrouillage	Oui

2.6.2 Mesures organisationnelles

Modalité	Applicabilité
Enregistrement des visiteurs à l'accueil	Oui
Système d'orientation et de surveillance des visiteurs	Oui
Règles et registre des clés (utilisation de codes de sécurité)	Oui

2.7 Contrôle d'accès logique

COSMO CONSULT sécurise l'utilisation des systèmes de traitement de données en mettant en œuvre différents contrôles d'accès de manière à ce que seules les personnes autorisées puissent y accéder. Chaque accès nécessite l'identification et l'authentification de l'utilisateur. Les accès extérieurs sont sécurisés par un pare-feu sur l'ensemble des sites.

2.7.1 Mesures techniques

Modalité	Applicabilité
Authentification par nom d'utilisateur et mot de passe	Oui
Utilisation du logiciel Endpoint Protection	Oui
Utilisation de pare-feu	Oui
Utilisation de la technologie VPN	Oui
Chiffrement du disque de données interne (disque dur interne)	Oui
Chiffrement des terminaux externes (mobiles) : clés USB, disques durs externes, DVD, etc.	Oui

2.7.2 Mesures organisationnelles

Modalité	Applicabilité
Gestion des utilisateurs et autorisations	Oui
Affectation/Règles de mot de passe	Oui
Profils utilisateur	Oui
Règles et registre des clés (utilisation de codes de sécurité)	Oui

2.8 Contrôle d'accès aux données

Les paragraphes suivants répertorient les mesures COSMO CONSULT qui garantissent que les personnes autorisées à utiliser un système de traitement de données peuvent uniquement accéder aux données qui leur sont communiquées et que les données à caractère personnel ne peuvent être consultées, copiées, modifiées, ni supprimées sans autorisation lors des opérations de traitement, d'utilisation et de stockage.

2.8.1 Mesures techniques

Modalité	Applicabilité
Utilisation de déchiqueteuses ou de conteneurs (systèmes d'élimination de fichiers)	Oui
Concept d'autorisation	Oui

2.8.2 Mesures organisationnelles

Modalité	Applicabilité
Concept d'autorisation (groupes AD, définition de rôles)	Oui
Politique de mot de passe (longueur et modification)	Oui
Gestion des droits d'utilisateur par les administrateurs système	Oui

2.9 Contrôle de transmission des données

Les paragraphes suivants répertorient les mesures COSMO CONSULT qui garantissent non seulement que les données à caractère personnel ne peuvent être consultées, copiées, modifiées, ni supprimées sans autorisation lors des transferts électroniques ou lors des transports/stockages sur des supports de données, mais aussi que ce critère peut être vérifié et validé au niveau du destinataire des données.

2.9.1 Mesures techniques

Modalité	Applicabilité
Journalisation des transferts de données	Client
Tunnel VPN (ligne sécurisée) sur le réseau COSMO CONSULT	Oui
Tunnel VPN (ligne sécurisée) sur le réseau du client	Client

2.9.2 Mesures organisationnelles

Modalité	Applicabilité
Sélection rigoureuse des employés	Oui
Règles d'usage des terminaux externes (mobiles)	Oui

2.10 Contrôle des entrées

Les paragraphes suivants répertorient les mesures COSMO CONSULT qui garantissent non seulement la possibilité de vérifier et de déterminer ultérieurement si des données à caractère personnel ont été saisies, modifiées ou supprimées des systèmes de traitement de données, mais permettent également de connaître l'auteur de ces opérations.

2.10.1 Fonctionnalités/remarques spécifiques

Les mesures techniques et organisationnelles relatives au contrôle des entrées doivent être adoptées côté client.
Ainsi, le client a la responsabilité d'affecter des noms d'utilisateurs plutôt que des connexions collectives pour des groupes d'employés ou des équipes (COSMO CONSULT est tenue d'accompagner le client dans cette démarche), mais aussi de journaliser les saisies, modifications et suppressions de données de manière à garantir la traçabilité de ces opérations au sein du système de production.

2.10.2 Mesures techniques

Modalité	Applicabilité
Journalisation des saisies, modifications et suppressions de données (protocole de modification ou équivalent)	Client

2.10.3 Mesures organisationnelles

Modalité	Applicabilité
Affectation des droits de saisie, modification et suppression des données sur la base d'un concept d'autorisation	Client
Traçabilité des saisies, modifications et suppressions de données par nom d'utilisateur (plutôt que par groupe d'utilisateurs)	Client

2.11 Contrôle des externalisations

Les paragraphes suivants répertorient les mesures COSMO CONSULT qui garantissent que le traitement des données à caractère personnel pour le compte de COSMO CONSULT par d'autres fournisseurs peut uniquement être réalisé conformément aux instructions du client. La liste des sous-traitants ultérieurs approuvés est régulièrement mise à jour à l'adresse https//www.cosmoconsult.com/data-protection. Les clients seront au préalable avertis par e-mail de toute modification de cette liste.

2.11.1 Mesures organisationnelles

Modalité	Applicabilité
Accords de traitement de données externalisé exclusivement écrits	Oui
Accords de traitement externalisé exclusivement écrits	Oui
Sélection des sous-traitants ultérieurs basée sur la diligence (notamment en termes de sécurité des données)	Oui
Obligation des employés du contractant en matière de confidentialité des données	Oui

2.12 Contrôle de la disponibilité

Les paragraphes suivants répertorient les mesures COSMO CONSULT qui garantissent que les données à caractère personnel sont protégées contre tout(e) dommage ou destruction accidentel(le) et qu'elles peuvent être rapidement rétablies en cas d'incident.

2.12.1 Fonctionnalités/remarques spécifiques

Les mesures techniques et opérationnelles en matière de disponibilité doivent être adoptées côté donneur d'ordre (client). Les mesures techniques et opérationnelles sont exclusivement réservées à un usage interne ou propre à COSMO CONSULT ; elles garantissent la capacité et l'accessibilité à des fins de travail.

2.12.2 Mesures techniques

Modalité	Applicabilité
Présence d'extincteurs d'incendie dans les salles de serveurs locales (ou à proximité)	Oui

2.12.3 Mesures organisationnelles

Modalité	Applicabilité
Conservation des sauvegardes de données en lieu sûr	Oui
Précautions de sauvegarde et de récupération	Oui

2.13 Contrôle de la séparation

Les paragraphes suivants répertorient les mesures qui garantissent que les données collectées à différentes fins peuvent être traitées séparément.

2.13.1 Mesures techniques

Modalité	Applicabilité
Séparation des systèmes de production et d'essai	Oui
Base de données avec séparation multitenant	Oui

2.13.2 Mesures organisationnelles

Modalité	Applicabilité
Définition de droits d'accès pour les différents clients	Oui

2.14 Contrôle de l'efficacité

Les paragraphes suivants répertorient les mesures qui garantissent que l'organisation interne des entreprises satisfait aux dispositions spéciales en matière de protection des données.

2.14.1 Mesures organisationnelles

Modalité	Applicabilité
Normes et réglementations en matière de sécurité informatique	Oui
Normes et réglementations en matière de sécurisation des stocks de données	Oui
Manuel d'organisation du site	Oui
Audits réguliers visant à évaluer la conformité aux mesures techniques et organisationnelles	Oui
Sessions de formation régulières	Oui

3. Délégué à la protection des données

2b Advice GmbH
Joseph-Schumpeter-Allee 25
53227 Bonn
Allemagne

Tél. : +49 (228) 92 61 65 123
Fax : +49 (228) 92 61 65 109

E-mail : cosmoconsult@2b-advice.com
Site web : http://www.2b-advice.com