Annexe 2[1]

Accord relatif au traitement en sous-traitance conformément à l'article 28, alinéa 3 du RGPD

[1]Annexe 2 L'accord sur le traitement externalisé conformément à l'article 28, paragraphe 3 du GDPR fait partie intégrante du contrat d'utilisation du RTC Vers. 2 – 01/26

Préambule

La présente annexe vient concrétiser les obligations des parties contractantes en matière de protection des données. Elle s'applique à toutes les activités liées au contrat/à la mission dans le cadre desquelles les employés du contractant ou les personnes mandatées par le contractant traitent des données à caractère personnel (« données ») du donneur d'ordre. Concrètement, le présent accord de traitement en sous-traitance régit les activités des services centraux pour le groupe d'entreprises.

§ 1 Objet, durée et spécification du traitement en sous-traitance

L'objet et la durée de la mission ainsi que la nature et la finalité du traitement ressortent du contrat ou de la mission. Plus précisément, les données énumérées à l'annexe 1 font notamment partie du traitement des données. Dans la mesure où celles-ci sont déjà régies par le contrat, l'annexe 1 n'est fournie qu'à titre d'information.

La durée de validité de cette annexe est fonction de la durée du contrat, à moins que les dispositions du présent accord relatif au traitement en sous-traitance et de l'annexe 1 du présent accord n'imposent des obligations allant au-delà.

§ 2 Champ d'application et responsabilité

(1) Le contractant traite des données à caractère personnel pour le compte du donneur d'ordre. Cela comprend les activités concrétisées dans le contrat, le mandat et/ou la spécification. Dans le cadre de ce contrat, le donneur d'ordre est seul responsable du respect des dispositions légales des lois sur la protection des données, en particulier de la légalité de la transmission des données au contractant ainsi que de la légalité du traitement des données (« responsable » au sens de l'article 4, alinéa 7 du RGPD).

(2) Les instructions sont d'abord déterminées par le contrat et peuvent ensuite être modifiées, complétées ou remplacées par le donneur d'ordre par écrit ou dans un format électronique (sous forme de texte) à l'endroit désigné par le contractant par des instructions individuelles (instruction unique). Les instructions non prévues dans le contrat seront traitées comme une demande de changement de service. Les instructions orales doivent être confirmées immédiatement par écrit ou sous forme de texte.

§ 3 Obligations du contractant

(1) Le contractant ne peut traiter les données des personnes concernées que dans le cadre de la mission et des instructions du donneur d'ordre, à moins qu'il ne s'agisse d'un cas exceptionnel au sens de l'article 28, alinéa 3 a) du RGPD. Le contractant informe immédiatement le donneur d'ordre s'il pense qu'une instruction enfreint des lois applicables. Le contractant peut suspendre l'exécution de l'instruction jusqu'à ce qu'elle ait été confirmée ou modifiée par le donneur d'ordre.

(2) Dans son domaine de responsabilité, le contractant doit concevoir l'organisation interne de manière à ce qu'elle réponde aux exigences particulières en matière de protection des données. Il doit prendre des mesures techniques et organisationnelles pour assurer une protection appropriée des données du donneur d'ordre, lesquelles satisfont aux exigences le Règlement général sur la protection (article 32 du RGPD).

Le contractant doit prendre les mesures techniques et organisationnelles qui garantissent sur la durée la confidentialité, l'intégrité, la disponibilité et la résilience à long terme des systèmes et services liés au traitement.

Le donneur d'ordre a connaissance de ces mesures techniques et organisationnelles et assume la responsabilité de veiller à ce qu'elles offrent un niveau de protection adéquat pour les risques liés aux données à traiter. Les mesures établies par le contractant sont énumérées à l'annexe 2 du présent accord de traitement des données en sous-traitance. Le contractant se réserve le droit de modifier les mesures de sécurité prises, tout en veillant à ce que toutes les mesures de sécurité soient conformes à l'état de la technique et à ce que le niveau de protection convenu contractuellement ne soit pas inférieur.

(3) Dans la mesure où il en a été convenu ainsi, le contractant aide le donneur d'ordre, dans la limite de ses possibilités, à répondre aux demandes et aux exigences des personnes concernées conformément au chapitre III du RGPD et à respecter les obligations citées dans les articles 33 à 36 du RGPD.

(4) Le contractant garantit qu'il est interdit aux employés chargés du traitement des données du donneur d'ordre et aux autres personnes travaillant pour le contractant de traiter les données en dehors du cadre des instructions. En outre, le contractant 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 de la mission.

(5) Le contractant informe immédiatement le donneur d'ordre s'il a connaissance d'une violation de la protection des données à caractère personnel du donneur d'ordre. Le contractant prend les mesures nécessaires pour sécuriser les données et atténuer les éventuelles conséquences négatives pour les personnes concernées et consulte immédiatement le donneur d'ordre à ce sujet.

(6) Le contractant informe le donneur d'ordre de l'interlocuteur pour les questions de protection des données qui se posent dans le cadre du contrat. Les données de contact sont mentionnées dans l'annexe 1 de cet accord.

(7) Le contractant garantit le respect de ses obligations en vertu de l'article 32, alinéa 1, lit. d), du RGPD, la mise en œuvre d'une procédure de contrôle régulier de l'efficacité des mesures techniques et organisationnelles visant à assurer la sécurité du traitement.

(8) Le contractant rectifie ou efface les données faisant l'objet du contrat si le donneur d'ordre lui 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, le contractant 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 donneur d'ordre ou restitue ces supports de données au donneur d'ordre, sauf si cela a déjà été convenu dans le contrat. Dans des cas particuliers, à déterminer par le donneur d'ordre, une conservation ou une remise a lieu. Le remboursement et les mesures de protection doivent être convenues séparément, sauf si cela a déjà été convenu dans le contrat.

(9) Les données, les supports de données ainsi que tout autre matériel doivent être restitués ou effacés à la demande du donneur d'ordre à la fin de la mission. Dans le cas de matériaux de test et de rebut, un mandat individuel n'est pas nécessaire. Si des frais supplémentaires sont occasionnés par des exigences différentes lors de la restitution ou de l'effacement des données, ils sont à la charge du donneur d'ordre.

(10) En cas de recours d'une personne concernée contre le donneur d'ordre concernant d'éventuelles revendications selon l'article 82 du RGPD, le contractant s'engage à soutenir le donneur d'ordre dans la défense de ces revendications dans la mesure de ses possibilités.

(11) L'exécution du traitement des données convenu dans le contrat a uniquement lieu dans un État membre de l'Union européenne ou dans un autre État contractant de l'accord sur l'Espace Économique Européen. Toute délocalisation dans un pays tiers requiert l'accord préalable du donneur d'ordre.

§ 4 Obligations du donneur d'ordre

(1) En cas d'erreurs ou d'irrégularités dans les résultats de la mission au regard des dispositions relatives à la protection des données, le donneur d'ordre est tenu d'en informer immédiatement le contractant sans rien omettre.

(2) En cas de recours par une personne concernée contre le donneur d'ordre concernant d'éventuelles revendications selon l'article 82 du RGPD, l'article 3, alinéa 10, s'applique en conséquence.

(3) Le donneur d'ordre informe le contractant de l'interlocuteur pour les questions de protection des données qui se posent dans le cadre du contrat. Les données de contact sont mentionnées dans l'annexe 1 de cet accord.

§ 5 Demandes de personnes concernées

(1) Si une personne concernée s'adresse au contractant avec des demandes de rectification, d'effacement ou de renseignement, le contractant renverra la personne concernée au donneur d'ordre, dans la mesure où une association au donneur d'ordre est possible selon les indications de la personne concernée. Le contractant transmettra immédiatement la demande de la personne concernée au donneur d'ordre. Le contractant assiste le donneur d'ordre dans la mesure de ses possibilités, sur instruction, dans la mesure où cela a été convenu. Le contractant n'est pas responsable si la requête de la personne concernée n'est pas satisfaite, n'est pas entièrement satisfaite ou n'est pas satisfaite en temps voulu par le donneur d'ordre.

§ 6 Possibilités de preuve et droits de contrôle

(1) Le contractant apporte au donneur d'ordre la preuve du respect des obligations énoncées dans ce contrat par des moyens adéquats.

(2) Après consultation avec le contractant, le donneur d'ordre a le droit d'effectuer des contrôles ou de faire effectuer des contrôles par des contrôleurs qu'il doit désigner au cas par cas. Ces contrôles sont effectués pendant les heures de bureau habituelles, sans perturber le fonctionnement de l'entreprise, après avoir prévenu et en tenant compte d'un délai de préparation raisonnable. Le contractant peut les soumettre à une notification préalable avec un délai de préparation raisonnable et à la signature d'une déclaration de confidentialité concernant les données d'autres clients et les mesures techniques et organisationnelles mises en place. Si le contrôleur mandaté par le donneur d'ordre se trouve dans une situation de concurrence par rapport au contractant, le contractant a alors un droit d'opposition contre celui-ci. Le contractant est en droit d'exiger une rémunération raisonnable pour l'assistance apportée lors de la réalisation d'une inspection. Le temps d'une inspection est en principe limité à un jour par année civile pour le contractant et le donneur d'ordre.

(3) Si une autorité de contrôle de la protection des données ou une autre autorité de contrôle compétente du donneur d'ordre procède à une inspection, l'alinéa 2 s'applique en principe par analogie. La signature d'une déclaration de confidentialité n'est pas nécessaire si cette autorité de contrôle est soumise à un devoir de discrétion professionnel ou légal dont la violation est sanctionnée par le Code pénal.

§ 7 Sous-traitants (autres contractants en sous-traitance)

(1) Le recours à des sous-traitants en tant qu'autres contractants en sous-traitance n'est autorisé que si le donneur d'ordre a donné son accord préalable.

(2) Il y a relation de sous-traitance soumise à autorisation lorsque le contractant confie à d'autres contractants la totalité ou une partie de la prestation convenue. Le contractant conclura des accords avec ces tiers dans la mesure nécessaire pour garantir des mesures appropriées de protection des données et de sécurité de l'information.

Le donneur d'ordre accepte que le contractant fasse appel à des sous-traitants. Les sous-traitants actifs au moment de la conclusion du présent accord sont énumérés à l'annexe 1. Avant de faire appel à des sous-traitants ou de les remplacer, le contractant en informe le donneur d'ordre (le cas échéant, délai et/ou dispositions pour les situations d'urgence). Le donneur d'ordre peut s'opposer à la modification - dans un délai raisonnable - pour des raisons importantes - auprès de l'organisme désigné par le donneur d'ordre. En l'absence de contestation dans le délai imparti, l'accord sur la modification est réputé acquis. En présence d'un motif important relevant de la protection des données et dans la mesure où il n'est pas possible de trouver une solution à l'amiable entre les parties, le donneur d'ordre et le contractant se voient accorder un droit de résiliation spécial.

(3) Si le contractant passe des commandes à des sous-traitants, il incombe au contractant de transmettre au sous-traitant ses obligations en matière de protection des données découlant du présent contrat.

(4) Le donneur d'ordre accepte que le contractant fasse appel à des entreprises liées au contractant pour l'exécution des prestations convenues par contrat ou qu'il sous-traite à des entreprises liées pour les prestations mentionnées. L'alinéa 3 s'applique également par analogie aux entreprises liées.

§ 8 Obligations d'information, clause relative à la forme écrite, choix du droit applicable

(1) Si des données du donneur d'ordre sont mises en danger chez le contractant par une saisie ou une confiscation, par une procédure d'insolvabilité ou de conciliation ou par tout autre évènement ou toute autre mesure de tiers, le contractant doit alors immédiatement en informer le donneur d'ordre. Le contractant informera immédiatement tous les responsables concernés que la souveraineté et la propriété des données appartiennent uniquement au donneur d'ordre en sa qualité de « responsable » dans le sens du RGPD.

(2) Les modifications et ajouts concernant cette annexe et toutes ses parties - les éventuelles garanties du contractant comprises - requièrent un accord écrit qui peut être passé en format électronique (sous forme de texte) ainsi que l'indication formelle selon laquelle il s'agit d'une modification ou d'un ajout concernant ces conditions. Il en va de même pour le renoncement à cette obligation de forme.

(3) En cas d'éventuelles oppositions, les règlementations de cette annexe relative à la protection des données prévalent sur les règlementations du contrat. L'éventuelle nullité de certaines parties de cette annexe n'affecterait en rien la validité du reste de l'annexe.

(4) C'est le droit allemand qui s'applique.

§ 9 Responsabilité et dommages-intérêts

Le donneur d'ordre et le contractant sont responsables vis-à-vis des personnes concernées conformément aux dispositions de l'article 82 du RGPD.

Annexe 1

Objet de la mission

L'objet de la mission comprend :
Mise à disposition d'un espace de stockage défini sur un serveur pour le stockage des données de clients

Durée du mandat

La durée du mandat dépend de la durée du contrat d'utilisation

Type de données

Les types / catégories de données suivantes font l'objet du traitement des données à caractère personnel :
Données de base à caractère personnel (noms, noms d'utilisateur, alias)
Données de communication (adresses e-mail, numéros de téléphone)
Fichiers journaux et fichiers log

Catégories de personnes concernées

Les catégories de personnes concernées par le traitement comprennent :
Utilisateur du portail

Sous-traitants

Nom et adresse	**Brève description de l'activité**
Modern Drive Technology GmbH Rettichstraße 7 92318 Neumarkt in der Oberpfalz	Mise à disposition d'un espace de stockage défini sur un serveur pour le stockage des données de clients

Responsable en matière de protection des données chez le contractant

Nom	**Adresse & contact**
Markus Olbring Responsable externe en matière de protection des données	comdatis it-consulting Deventer Weg 8, 48683 Ahaus Téléphone : 02561-7569986 ou 0173-9799897 E-mail : datenschutz@ruthmann.de

*S'il n'y a pas d'obligation de désigner un responsable à la protection des données, un interlocuteur pour les questions de protection des données doit être désigné.

Annexe 2

Description	Mesure	Oui	Non	Non pertinent
Contrôle d'accès	L'entreprise dispose d'une zone d'accueil centralisée et occupée.	x		
	L'entreprise dispose d'un système de contrôle d'accès, c'est-à-dire d'une sécurisation des portes par un ouvre-porte, un lecteur de badge, un système de fermeture automatique ou similaire.	x		
	Les locaux de l'entreprise sont toujours fermés à clé.		x	
	Il existe un système de contrôle d'accès pour les personnes étrangères à l'entreprise.	x		
	Une gestion centrale des clés est établie dans l'entreprise pour la remise de clés.	x		
	Une liste des clés est tenue à un poste central, qui indique quel collaborateur a reçu une clé et quand.	x		
	Les collaborateurs sont tenus par écrit de signaler immédiatement la perte d'une clé.	x		
	Les visiteurs reçoivent un badge d'accès et le rendent lorsqu'ils quittent l'entreprise.		x	
	L'accès aux salles de serveurs est limité aux collaborateurs autorisés.	x		
	Les salles de serveurs sont toujours fermées à clé.	x		
	Les accès aux salles de serveurs sont consignés.	x		
	Le bâtiment est protégé par une alarme.		x	
	Le bâtiment se trouve sur un terrain clôturé.	x		
	Une surveillance du bâtiment est assurée par vidéo, par un gardien d'usine ou par un gardien de nuit/garde.	x		
Contrôle d'accès	Les collaborateurs reçoivent des noms d'utilisateur et des mots de passe individuels pour la connexion au poste de travail PC.		x	
	Les mots de passe initiaux doivent être modifiés par l'utilisateur.	x		
	Les mots de passe doivent être modifiés régulièrement.	x		
	Les mots de passe ont des exigences de complexité (p. ex. chiffres, lettres, caractères spéciaux).	x		
	Les mots de passe doivent comporter au moins 8 caractères.	x		
	Les mots de passe administratifs doivent comporter au moins 12 caractères.	x		
	Des procédures d'authentification à deux facteurs sont utilisées comme alternative aux modifications régulières des mots de passe.	x		
	Les postes de travail PC sont automatiquement verrouillés en cas d'inactivité et ne peuvent être déverrouillés que par la saisie d'un mot de passe.	x		
	Les réseaux internes sont protégés contre les accès non autorisés de l'extérieur par un pare-feu.	x		
	Les accès externes aux réseaux internes ne sont possibles que via des connexions cryptées (par ex. VPN).	x		
	Les supports de données des terminaux mobiles (ordinateurs portables, smartphones, tablettes) sur lesquels se trouvent des données à caractère personnel sont cryptés.	x		
	Les postes de travail PC et les ordinateurs portables disposent d'une protection antivirus.	x		
Contrôle d'accès	Un concept d'autorisation est disponible dans l'entreprise et contient des niveaux d'autorisation différenciés.		x	

	Les profils d'utilisateurs garantissent dans les applications que les collaborateurs ne disposent que des droits nécessaires à l'accomplissement de leurs missions.	x		
	Les ports USB des postes de travail PC sont bloqués ou soumis à une surveillance technique.	x		
	Les graveurs des postes de travail PC sont bloqués ou soumis à une surveillance technique.	x		
	Les collaborateurs sont tenus d'utiliser exclusivement les supports de données externes fournis par l'entreprise.	x		
	Les supports de données informatiques qui ne sont plus utilisés sont éliminés dans le respect de la protection des données.	x		
	Les droits administratifs ne sont disponibles que pour les collaborateurs autorisés.	x		
Principe de séparation	Les données à caractère personnel collectées à des fins différentes sont conservées séparément.	x		
	Les applications permettent une séparation logique des clients.	x		
	Une séparation des clients est mise en œuvre par le biais du concept d'autorisation implémenté.	x		
	L'entreprise fait la distinction entre le système de production et le système de test.	x		
	Les données de différents projets / donneurs d'ordre sont, dans la mesure du possible, traitées séparément.	x		
	Dans le cas de données pseudonymisées, il est garanti qu'il existe une séparation du fichier d'attribution aux données.		x	
Contrôle de la transmission	L'entreprise dispose de procédures permettant l'échange crypté de données à caractère personnel (par ex. cryptage du courrier électronique, SFTP, https).	x		
	Lors de l'envoi de données à caractère personnel (p. ex. par e-mail), les collaborateurs sont tenus par écrit d'envoyer ces données sous forme cryptée.		x	
	En outre, des instructions de travail, un accord d'entreprise ou une directive obligent les collaborateurs à ne pas partager de données à caractère personnel via des services non sécurisés ou non conformes à la protection des données (par exemple, pas de partage de données via les médias sociaux, WhatsApp, des services de stockage en clouds privés ou gratuits).	x		
Contrôle des saisies	La traçabilité de la saisie, de la modification et de la suppression des données à caractère personnel est assurée par le système grâce à une consignation (qui ? Quand ?).		x	
	En cas d'utilisation d'un logiciel standard, il est garanti que des consignations suffisantes et conformes aux exigences de protection des données sont activées.		x	
Contrôle de la disponibilité	Un concept d'urgence documenté est disponible dans l'entreprise.	x		
	Des exercices d'urgence sont régulièrement organisés.		x	
	Une protection multiple des serveurs et des données est mise en place.	x		
	Les salles de serveurs disposent d'une alimentation électrique sans interruption (ASI) appropriée.		x	
	Les salles de serveurs disposent de systèmes de climatisation multiples.	x		

	Les salles de serveurs sont équipées de détecteurs de fumée.	x		
	Des dispositifs d'extinction d'incendie se trouvent dans ou devant les salles de serveurs.	x		
	Les salles des serveurs disposent d'un capteur pour le système d'alarme.		x	
	Des messages d'alarme sont émis en cas d'accès non autorisé aux salles de serveurs.		x	
	Les sauvegardes des données sont conservées dans un endroit sûr et délocalisé.	x		
	Les données sont régulièrement sauvegardées dans le cadre de scénarios de test.		x	
	Des antivirus sont installés sur les terminaux dans toute l'entreprise.	x		
	Les scanners antivirus se mettent à jour automatiquement.	x		
	Les systèmes d'exploitation des postes de travail clients sont régulièrement mis à jour.	x		
	Les systèmes d'exploitation sur les serveurs sont régulièrement mis à jour.	x		
	L'entreprise a mis en place des procédures qui garantissent une mise à jour régulière, y compris pour les programmes auxiliaires (par ex. lecteurs PDF, programmes zip, Java, Flash).		x	
	L'entreprise dispose de directives contraignantes pour la maintenance et l'exécution des mises à jour		x	
	Grâce à un monitoring automatique et permanent permettant de détecter les dysfonctionnements, les erreurs éventuelles sont rapidement signalées.	x		
	Les systèmes informatiques critiques de l'entreprise, en particulier ceux qui sont accessibles via Internet, sont soumis à des tests de vulnérabilité.		x	
	Les systèmes de pare-feu et de routeurs sont régulièrement mis à jour (mise à jour du micrologiciel).	x		
Contrôle de l'ordre	Le choix des prestataires de services externes se fait avec le plus grand soin (notamment en ce qui concerne la protection des données et la sécurité de l'information).	x		
	En cas de recours à des prestataires de services externes, il est garanti que le traitement des données n'a pas lieu en dehors de l'UE ou d'un pays tiers sûr.	x		
	Des dispositions contractuelles ont été prises avec les prestataires de services externes qui traitent des données à caractère personnel ou qui pourraient les consulter dans le cadre de leur activité, dans le respect des dispositions de l'article 28 du règlement général sur la protection des données.	x		
	En cas de recours à des prestataires de services externes qui traitent des données à caractère personnel, il est garanti qu'il existe une base juridique pour le traitement (p. ex. accord sur le traitement des données en sous-traitance, clauses contractuelles types de l'UE).	x		
	Des procédures sont mises en place pour garantir que les données à caractère personnel sont détruites ou effacées à la fin de la mission. Les éventuels délais de conservation légaux sont pris en compte et respectés.	x		
	Des droits de contrôle sont convenus dans les dispositions contractuelles avec les prestataires de services externes.	x		

	Les droits de contrôle convenus sont exercés à intervalles réguliers (par ex. en demandant une confirmation, un rapport)		x	
	Les prestataires de services externes sont tenus au secret professionnel.	x		
Gestion de la protection des données	Un responsable en matière de protection des données est désigné par écrit dans l'entreprise.	x		
	Il n'existe aucune obligation légale de désigner un responsable en matière de protection des données.			x
	Par le biais d'une ligne directrice sur la protection des données et la sécurité de l'information, la direction a informé tous les collaborateurs de la nécessité de protéger les données.	x		
	Il existe dans l'entreprise des prescriptions écrites (par exemple une directive, des accords d'entreprise) concernant le traitement des données et les systèmes informatiques.		x	
	Les collaborateurs sont tenus par écrit au secret professionnel.	x		
	Les collaborateurs sont sensibilisés à la protection des données dans le cadre de formations.		x	
	L'entreprise dispose d'un registre documenté des activités de traitement. Si nécessaire, les activités de traitement en sous-traitance y sont également documentées.	x		
	L'entreprise dispose d'une documentation sur les mesures de sécurité des activités de traitement (dite TOM)		x	
	Des contrôles réguliers permettent de s'assurer que les mesures établies pour respecter la protection des données sont appropriées.		x	
	Le responsable en matière de protection des données rédige un rapport annuel.	x		
	L'entreprise dispose d'une certification dans le domaine de la sécurité de l'information (par ex. ISO/IEC 27001, IDW PS 951, VdS 3473).		x	
	L'entreprise dispose d'une certification dans le domaine de la protection des données.		x	