Contrat de sous-traitance des données ATLAS.ti

Préambule

Le présent contrat de sous-traitance des données régit le traitement de données pour le compte du client par ATLAS.ti Scientific Software Development GmbH en qualité de sous-traitant. Il fait partie intégrante du contrat concerné par renvoi dans les conditions d'utilisation.

Définitions

1.1 Conformément à l'art. 4, point 7 du RGPD, le « responsable du traitement » est l'organisme qui, seul ou conjointement avec d'autres responsables du traitement, décide des finalités et des moyens du traitement des données à caractère personnel.

1.2 Conformément à l'art. 4, point 8 du RGPD, le « sous-traitant » est une personne physique ou morale, une autorité publique, un service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

1.3 Conformément à l'art. 4, point 1 du RGPD, on entend par « données à caractère personnel » toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

1.4 Les « données à caractère personnel particulièrement sensibles » sont les données à caractère personnel visées à l'art. 9 du RGPD, dont peuvent être déduites l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes concernées, les données à caractère personnel visées à l'art. 10 du RGPD relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes, ainsi que les données génétiques au sens de l'art. 4, point 13 du RGPD, les données biométriques au sens de l'art. 4, point 14 du RGPD, les données concernant la santé au sens de l'art. 4, point 15 du RGPD et les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

1.5 Conformément à l'art. 4, point 2 du RGPD, le « traitement » désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

1.6 Conformément à l'art. 4, point 21 du RGPD, l'« autorité de contrôle » est une autorité publique indépendante instituée par un État membre en vertu de l'art. 51 du RGPD.

Objet

2.1 Le prestataire fournit au client des prestations dans le domaine de la « mise à disposition de logiciels » sur la base du contrat principal conclu entre les parties. Dans le cadre du contrat principal, le prestataire se voit accorder l'accès à des données à caractère personnel et traite ces données exclusivement pour le compte et sur instruction du client. L'objet du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées sont définis à l'annexe 1 du présent contrat de sous-traitance des données. Il incombe au client d'apprécier la licéité du traitement des données.

2.2 Les parties concluent le présent contrat de sous-traitance des données afin de préciser les droits et obligations réciproques en matière de protection des données. En cas de doute, les dispositions du présent contrat prévalent sur celles du contrat principal.

2.3 Les dispositions du présent contrat de sous-traitance des données s'appliquent à toutes les activités liées au contrat principal dans le cadre desquelles le prestataire et ses salariés ou les auxiliaires mandatés par lui entrent en contact avec des données à caractère personnel provenant du client ou collectées pour son compte.

2.4 Le présent contrat de sous-traitance des données prend effet à sa signature ; la durée du présent contrat de sous-traitance des données est fonction de la durée du contrat principal, sauf si les dispositions suivantes imposent des obligations ou des droits de résiliation allant au-delà.

Instructions

3.1 Le prestataire ne peut collecter, traiter ou utiliser des données que dans le cadre du contrat principal et conformément aux instructions du client ; cela s'applique en particulier au transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale. Si le droit de l'Union européenne ou des États membres auquel le prestataire est soumis exige un traitement ultérieur, le prestataire informe le client de ces exigences légales avant le traitement.

3.2 Les instructions du client résultent initialement du présent contrat et peuvent ensuite être modifiées, complétées ou remplacées par des instructions individuelles données par écrit ou sous forme de texte (instructions individuelles). Le client est en droit de donner à tout moment les instructions correspondantes. Cela comprend les instructions relatives à la rectification, à l'effacement et au blocage des données. Les instructions orales doivent être confirmées sans délai par écrit ou sous forme de texte.

3.3 Toutes les instructions données doivent être documentées tant par le client que par le prestataire. Les instructions qui vont au-delà de la prestation convenue dans le contrat principal sont traitées comme une demande de modification de la prestation.

3.4 Si le prestataire estime qu'une instruction du client enfreint la réglementation relative à la protection des données, il doit en informer le client sans délai. Le prestataire est en droit de suspendre l'exécution de l'instruction en question jusqu'à sa confirmation ou sa modification par le client. Le prestataire peut refuser d'exécuter une instruction manifestement illicite.

Catégories de données, personnes concernées

Dans le cadre de l'exécution du contrat principal, le prestataire se voit accorder l'accès aux données à caractère personnel précisées à l'**annexe 1**. Les personnes concernées par le traitement des données sont également définies à l'**annexe 1**.

Obligations du prestataire

5.1 Le prestataire est tenu de respecter les dispositions légales relatives à la protection des données et de ne pas transmettre à des tiers les informations obtenues de la sphère du client ni de leur en donner l'accès. Les documents et les données doivent être protégés contre tout accès non autorisé, compte tenu de l'état de la technique.

5.2 Dans son domaine de responsabilité, le prestataire organise sa structure interne de manière à satisfaire aux exigences particulières de la protection des données. Le prestataire prend toutes les mesures techniques et organisationnelles nécessaires à la protection appropriée des données du client conformément à l'art. 32 du RGPD, en particulier au moins les mesures énumérées à l'annexe 2. Le prestataire se réserve le droit de modifier les mesures de sécurité adoptées, en veillant à ce que le niveau de protection convenu contractuellement ne soit pas compromis.

5.3 Il est interdit aux personnes employées par le prestataire au traitement des données de collecter, de traiter ou d'utiliser des données à caractère personnel sans autorisation. Le prestataire impose une obligation correspondante à toutes les personnes qu'il charge du traitement et de l'exécution du présent contrat (ci-après dénommées « salariés ») (obligation de confidentialité, art. 28, paragraphe 3, point b) du RGPD) et veille avec la diligence requise au respect de cette obligation. Ces obligations doivent être formulées de manière à rester en vigueur après la fin du présent contrat ou de la relation de travail entre le salarié et le prestataire. Sur demande, des justificatifs appropriés de ces obligations doivent être fournis au client de manière adéquate.

Obligations d'information du prestataire

6.1 En cas de dysfonctionnements, de soupçon de violation de la protection des données ou de manquement aux obligations contractuelles de la part du prestataire, de soupçon d'incidents de sécurité ou d'autres irrégularités dans le traitement des données à caractère personnel par le prestataire, par des personnes employées par lui dans le cadre de la commande ou par des tiers, le prestataire informe le client sans délai par écrit ou sous forme de texte. Il en va de même des contrôles du prestataire par une autorité de contrôle de la protection des données. La notification d'une violation de données à caractère personnel contient au moins les informations suivantes :

a) une description de la nature de la violation de données à caractère personnel, y compris, dans la mesure du possible, les catégories et le nombre de personnes concernées, ainsi que les catégories et le nombre d'enregistrements de données à caractère personnel concernés
b) une description des mesures prises ou proposées par le prestataire pour remédier à la violation et, le cas échéant, des mesures visant à atténuer ses éventuelles conséquences négatives

6.2 Le prestataire prend sans délai les mesures nécessaires pour sécuriser les données et atténuer les éventuelles conséquences négatives pour les personnes concernées, en informe le client et sollicite de nouvelles instructions.

6.3 En outre, le prestataire est tenu de fournir à tout moment des informations au client dans la mesure où les données du client sont concernées par une violation au sens du point 6.1.

6.4 Si les données du client détenues par le prestataire sont mises en péril par une saisie ou une confiscation, par une procédure d'insolvabilité ou de concordat, ou par d'autres événements ou mesures de tiers, le prestataire doit en informer le client sans délai, sauf si cela lui est interdit par décision judiciaire ou administrative. Dans ce contexte, le prestataire informe sans délai toutes les autorités compétentes que le pouvoir de décision sur les données appartient exclusivement au client en sa qualité de responsable du traitement.

6.5 Le prestataire informe le client sans délai de toute modification substantielle des mesures de sécurité visées au point 5.2.

6.6 Le client doit être informé sans délai de tout changement de la personne du délégué à la protection des données/de l'interlocuteur en matière de protection des données.

6.7 Le prestataire et, le cas échéant, son représentant tiennent un registre des activités de traitement effectuées pour le compte du client, contenant toutes les informations exigées par l'art. 30, paragraphe 2 du RGPD. Ce registre est mis à la disposition du client sur demande.

6.8 Le prestataire coopère dans une mesure appropriée à l'établissement du registre des procédures par le client. Le prestataire doit fournir au client les informations nécessaires de manière adéquate.

Droits de contrôle du client

7.1 Le client a le droit de vérifier à tout moment, dans la mesure nécessaire, que le prestataire respecte les dispositions légales relatives à la protection des données et/ou les dispositions contractuelles convenues entre les parties et/ou que le prestataire se conforme aux instructions du client. Le prestataire est en droit de démontrer le respect des obligations prévues au présent contrat de sous-traitance des données par des moyens appropriés, y compris des auto-évaluations, des certificats, etc.

7.2 Le prestataire est tenu de fournir des informations au client dans la mesure où cela est nécessaire à la réalisation du contrôle défini au paragraphe 1 ci-dessus.

7.3 Si cela est nécessaire dans des cas particuliers, le client peut exiger la consultation des données traitées par le prestataire pour son compte ainsi que des systèmes et programmes de traitement des données utilisés.

7.4 Après notification préalable et moyennant un délai de préavis raisonnable, le client peut effectuer le contrôle au sens du paragraphe 1 dans les locaux du prestataire pendant les heures normales d'ouverture. Le client veille à ce que les contrôles ne soient effectués que dans la mesure nécessaire, afin de ne pas perturber de manière disproportionnée l'activité du prestataire. Les parties partent du principe qu'un contrôle est nécessaire au maximum une fois par an. Les contrôles supplémentaires doivent être motivés par le client, avec indication du motif. En cas de contrôles sur place, le client rembourse au prestataire, dans une mesure raisonnable, les frais engagés, y compris les frais de personnel, pour l'encadrement et l'accompagnement des contrôleurs sur place. Les bases de calcul des coûts sont communiquées au client par le prestataire avant la réalisation du contrôle. Le prestataire peut subordonner les contrôles à une notification préalable dans un délai approprié et à la signature d'un accord de confidentialité. Si le contrôleur mandaté par le client se trouve dans une situation de concurrence avec le prestataire, celui-ci dispose d'un droit d'opposition.

7.5 Au choix du prestataire, la preuve du respect des mesures techniques et organisationnelles peut également être apportée, au lieu d'un contrôle sur place, par la production d'un certificat d'audit approprié et à jour, de rapports ou d'extraits de rapports d'organismes indépendants (par ex. commissaires aux comptes, audit interne, délégué à la protection des données, service de sécurité informatique, auditeurs en protection des données ou auditeurs qualité) ou par une certification appropriée, si le rapport d'audit permet au client de s'assurer de manière raisonnable que les mesures techniques et organisationnelles prévues à l'annexe 2 du présent contrat de sous-traitance des données sont respectées. Si le client a des doutes fondés quant à la pertinence du document de contrôle au sens de la première phrase, un contrôle sur place peut être effectué par le client. Le client est conscient qu'un contrôle sur place dans les centres de données n'est pas possible ou n'est possible que dans des cas exceptionnels justifiés.

7.6 En cas de mesures prises par l'autorité de contrôle à l'encontre du client au sens de l'art. 58 du RGPD, notamment en ce qui concerne les obligations d'information et de contrôle, le prestataire est tenu de fournir au client les informations nécessaires et de permettre à l'autorité de contrôle compétente de procéder à un contrôle sur place. Le client est informé par le prestataire des mesures correspondantes envisagées.

7.7 Le prestataire prouve au client, sur demande, l'engagement des salariés conformément au point 5.3.

Recours à des sous-traitants ultérieurs et transfert de données

8.1 Le prestataire est en droit de recourir à des sous-traitants ultérieurs pour le traitement des données du client. Le prestataire doit sélectionner soigneusement les sous-traitants ultérieurs et vérifier, avant l'attribution de la commande, qu'ils sont en mesure de respecter les accords conclus entre le client et le prestataire. En particulier, le prestataire vérifie au préalable et régulièrement pendant la durée du contrat que le sous-traitant ultérieur a pris les mesures techniques et organisationnelles requises par l'art. 32 du RGPD pour la protection des données à caractère personnel.

8.2 Le client accepte que le prestataire recoure à d'autres sous-traitants ultérieurs ou remplace des sous-traitants ultérieurs si nécessaire. Le prestataire informe le client de ces changements dans un délai raisonnable à l'avance sous forme électronique. Le client peut s'opposer au changement pour un motif légitime dans un délai raisonnable fixé par le prestataire selon son appréciation équitable. À défaut d'opposition dans ce délai, le consentement au changement est réputé donné.

8.3 Le prestataire est tenu d'obtenir du sous-traitant ultérieur la confirmation que celui-ci a désigné un délégué à la protection des données conformément à l'art. 37 du RGPD, dans la mesure où le sous-traitant ultérieur est légalement tenu de désigner un délégué à la protection des données.

8.4 Le prestataire veille à ce que les dispositions convenues dans le présent contrat de sous-traitance des données ainsi que toute instruction complémentaire du client s'appliquent également au sous-traitant ultérieur.

8.5 Le prestataire est notamment tenu de garantir par des dispositions contractuelles que les droits de contrôle du client et des autorités de contrôle s'appliquent également au sous-traitant ultérieur et que des

droits de contrôle correspondants soient convenus au profit du client et des autorités de contrôle. En outre, il doit être stipulé dans le contrat que le sous-traitant ultérieur doit tolérer ces mesures de contrôle et les éventuels contrôles sur place.

8.6 Ne sont pas considérés comme des relations de sous-traitance ultérieure au sens des paragraphes 1 à 5 les services que le prestataire obtient de tiers à titre de prestation purement accessoire pour l'exercice de son activité commerciale. En font partie, par exemple, les services de nettoyage, les services de télécommunications purs sans lien spécifique avec les prestations que le prestataire fournit au client, les services postaux et de messagerie, les services de transport et les services de gardiennage. Le prestataire est néanmoins tenu de s'assurer, également dans le cas de prestations accessoires fournies par des tiers, que des précautions appropriées et des mesures techniques et organisationnelles ont été prises pour assurer la protection des données à caractère personnel. La maintenance et l'entretien de systèmes informatiques ou d'applications constituent une relation de sous-traitance ultérieure et un traitement de données sur instruction au sens de l'art. 28 du RGPD soumis à autorisation, lorsque la maintenance et les tests portent sur des systèmes informatiques qui sont également utilisés dans le cadre de la fourniture de prestations au client et lorsque des données à caractère personnel traitées pour le compte du client sont accessibles lors de la maintenance.

8.7 Le client reconnaît et accepte que le prestataire puisse transférer et traiter les données du client vers et dans des pays tiers, y compris des pays situés en dehors de l'EEE sans décision d'adéquation de la Commission européenne, auprès de ses sous-traitants ultérieurs, à savoir OpenAI LLC, 3180 18th St, San Francisco, Californie, 94110, États-Unis (fonctions d'analyse par IA génératives) et Deepgram, Inc., San Francisco, Californie, États-Unis (transcription d'enregistrements audio et vidéo) et/ou d'autres fournisseurs d'IA. Le prestataire veille à ce que ces transferts soient effectués conformément au droit applicable en matière de protection des données et au présent contrat de sous-traitance des données. En particulier, le prestataire conclut des clauses contractuelles types conformément à l'art. 46, paragraphe 2, point c) du RGPD ou d'autres garanties appropriées (telles que des règles d'entreprise contraignantes conformément à l'art. 47 du RGPD). Lorsqu'un sous-traitant ultérieur est certifié au titre d'une décision d'adéquation prise en vertu de l'art. 45 du RGPD, telle que le cadre de protection des données UE–États-Unis, le transfert peut également être

fondé sur cette décision d'adéquation ; les clauses contractuelles types demeurent en place à titre de garantie subsidiaire.

Traitement aux fins des fonctions d'IA

9.1 Lorsque le client utilise des fonctions du logiciel assistées par IA (y compris le codage automatisé, les résumés, l'analyse conversationnelle de documents et la transcription), le prestataire traite les contenus transmis par le client exclusivement aux fins de fournir la fonction demandée. Ni le prestataire ni, en vertu des accords conclus par lui, ses sous-traitants ultérieurs n'utilisent ces contenus pour entraîner, réentraîner ou améliorer des modèles d'intelligence artificielle. Les sous-traitants ultérieurs d'IA du prestataire ne conservent les contenus transmis que temporairement, dans la mesure nécessaire à la fourniture du service et à la détection des abus ; sur demande, le prestataire informe le client des durées de conservation actuellement applicables chez ses sous-traitants ultérieurs d'IA.

9.2 Le prestataire fournit au client, sur demande raisonnable, les informations relatives aux fonctions assistées par IA dont le client a raisonnablement besoin pour se conformer à ses propres obligations au titre du règlement (UE) 2024/1689 (règlement sur l'IA), en particulier les obligations de transparence. Les obligations légales d'information du prestataire demeurent inchangées.

Droits des personnes concernées

10.1 Le client est seul responsable de la sauvegarde des droits des personnes concernées. Le prestataire assiste le client, dans la mesure du possible, par des mesures techniques et organisationnelles appropriées, dans l'exécution des obligations du client au titre des art. 12 à 22 ainsi que 32 et 36 du RGPD.

10.2 Si une personne concernée fait valoir des droits, tels que le droit d'accès/à l'information, de rectification ou d'effacement de ses données, directement auprès du prestataire, celui-ci ne réagit pas de manière autonome, mais renvoie la personne concernée sans délai au client et attend les instructions de ce dernier.

Obligations de confidentialité

11.1 Les deux parties s'engagent à traiter comme confidentielles, sans limitation de durée, toutes les informations reçues dans le cadre de l'exécution du présent contrat de sous-traitance des données et à ne les utiliser qu'aux fins de l'exécution du présent contrat de sous-traitance des

données et/ou du contrat principal. Aucune des parties n'est en droit d'utiliser ces informations, en tout ou en partie, à d'autres fins que celles qui viennent d'être mentionnées ni de les mettre à la disposition de tiers.

11.2 L'obligation qui précède ne s'applique pas aux informations que l'une des parties a manifestement obtenues de tiers sans être tenue au secret ou qui sont connues du public.

Fin du contrat

Après la fin du contrat principal ou à tout moment à la demande du client, le prestataire doit restituer au client tous les documents, données et supports de données qui lui ont été remis ou – à la demande du client et sauf obligation de conserver les données à caractère personnel en vertu du droit de l'Union ou du droit de la République fédérale d'Allemagne – les effacer. L'effacement doit être documenté de manière appropriée et prouvé sur demande.

Dispositions finales

13.1 Les parties conviennent que l'exception de droit de rétention par le prestataire (au titre du § 273 du Code civil allemand, BGB) concernant les données à traiter et les supports de données associés est exclue.

13.2 Les modifications et compléments apportés au présent contrat de sous-traitance des données et à l'ensemble de ses éléments – y compris toute assurance donnée par le prestataire – requièrent un accord écrit, qui peut également revêtir une forme électronique (forme de texte), ainsi que l'indication expresse qu'il s'agit d'une modification ou d'un complément au présent contrat de sous-traitance des données. Cela s'applique également à la renonciation à cette exigence de forme.

13.3 Si certaines dispositions du présent contrat sont ou deviennent nulles ou inapplicables, en tout ou en partie, la validité des autres dispositions n'en est pas affectée.

13.4 Le présent contrat est soumis au droit allemand.

Annexes :
Annexe 1 : Description du traitement
Annexe 2 : Mesures techniques et organisationnelles

Annexe 1 : Description du traitement

1. Portée et finalité du traitement
La commande du client au prestataire comprend les travaux et/ou

prestations suivants :
Mise à disposition de la plateforme d'analyse de données du prestataire en mode SaaS, services d'intelligence artificielle, y compris les fonctions d'analyse assistées par IA (codage automatisé, résumés, analyse conversationnelle de documents) et la transcription assistée par IA d'enregistrements audio et vidéo

2. Type(s) de données à caractère personnel
Les types de données suivants font régulièrement l'objet du traitement des données :
Données que le client analyse ou traite à l'aide de la plateforme d'analyse de données du prestataire et dont la nature est déterminée par le client à sa propre discrétion, et qui peuvent notamment comprendre, par exemple, des données relatives aux entités et projets du client, aux personnes testées, aux patients et aux autres participants et personnes concernées dans le cadre d'études scientifiques et de projets de recherche. Enregistrements vocaux et vidéo téléchargés par le client à des fins de transcription, ainsi que les transcriptions qui en sont issues ; le traitement des enregistrements vocaux est limité à la transcription, et il n'est procédé à aucune identification du locuteur ni à aucune analyse biométrique au sens de l'art. 4, point 14 et de l'art. 9, paragraphe 1 du RGPD.

3. Catégories de données
Données concernées par le traitement des données :
Catégories de données que le client analyse ou traite à l'aide de la plateforme d'analyse de données du prestataire et dont les catégories sont déterminées par le client à sa propre discrétion, et qui peuvent comprendre, par exemple, les catégories de données suivantes : prénom et nom, coordonnées, données médicales, données génétiques, données biométriques, autres catégories particulières de données à caractère personnel, données relatives aux habitudes de vie et à d'autres circonstances, informations issues d'entretiens, retours de clients et données comportementales.

4. Catégories de personnes concernées
Personnes concernées par le traitement des données :
Personnes testées, patients, participants à des recherches ou personnes interrogées, salariés, autres participants et personnes concernées dans le cadre d'études ou de projets de recherche, toute personne physique figurant dans les contenus analysés par le client.

Annexe 1 : Description du traitement

1. Portée et finalité du traitement
   La commande du client au prestataire comprend les travaux et/ou prestations suivants :
   Mise à disposition de la plateforme d'analyse de données du prestataire en mode SaaS, services d'intelligence artificielle

2. Type(s) de données à caractère personnel
   Les types de données suivants font régulièrement l'objet du traitement des données :
   Données que le client analyse ou traite à l'aide de la plateforme d'analyse de données du prestataire et dont la nature est déterminée par le client à sa propre discrétion, et qui peuvent notamment comprendre, par exemple, des données relatives aux entités et projets du client, aux personnes testées, aux patients et aux autres participants et personnes concernées dans le cadre d'études scientifiques et de projets de recherche.

3. Catégories de personnes concernées
   Personnes concernées par le traitement des données :
   Catégories de données que le client analyse ou traite à l'aide de la plateforme d'analyse de données du prestataire et dont les catégories sont déterminées par le client à sa propre discrétion, et qui peuvent comprendre, par exemple, les catégories de données suivantes : prénom et nom, coordonnées, données médicales, données génétiques, données biométriques, autres catégories particulières de données à caractère personnel, données relatives aux habitudes de vie et à d'autres circonstances, informations issues d'entretiens, retours de clients et données comportementales.

Annexe 2 : Mesures techniques et organisationnelles
1. Confidentialité (art. 32, paragraphe 1, point b) du RGPD)

a. Contrôle de l'accès physique
Mesures propres à empêcher les personnes non autorisées d'accéder aux installations de traitement de données avec lesquelles des données à caractère personnel sont traitées ou utilisées :
• Système de fermeture à serrure à code
• Serrures de sûreté
• Gestion des clés (remise des clés, etc.)
• Enregistrement des visiteurs
• Sélection rigoureuse du personnel de sécurité

• Sélection rigoureuse du personnel de nettoyage
• Système de fermeture manuel

b. Contrôle de l'accès aux systèmes
Mesures propres à empêcher que les systèmes de traitement de données soient utilisés par des personnes non autorisées :
• Attribution de droits d'utilisateur
• Attribution de mots de passe
• Authentification par nom d'utilisateur / mot de passe
• Utilisation d'un logiciel antivirus
• Utilisation d'un pare-feu logiciel

c. Contrôle de l'accès aux données
Mesures garantissant que les personnes autorisées à utiliser un système de traitement de données ne peuvent accéder qu'aux données relevant de leur autorisation d'accès et que les données à caractère personnel ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation lors du traitement, de l'utilisation et après leur conservation :
• Gestion des droits par l'administrateur système
• Nombre d'administrateurs réduit au strict minimum
• Journalisation des accès aux applications, en particulier lors de la saisie, de la modification et de la suppression de données
• Destruction en règle des supports de données (DIN 32757)
• Recours à des destructeurs de documents ou à des prestataires de services
• Journalisation de la destruction

d. Contrôle de la séparation
Mesures garantissant que les données collectées à des fins différentes peuvent être traitées séparément :
• Stockage logiquement strictement séparé des données dans différents systèmes clients
• Chiffrement des enregistrements de données traités à la même finalité
• Attribution aux enregistrements d'attributs de finalité/de champs de données
• Séparation des systèmes de production et de test

2. Intégrité (art. 32, paragraphe 1, point b) du RGPD)
a. Contrôle de la transmission
Mesures garantissant que les données à caractère personnel ne peuvent être lues, copiées, modifiées ou supprimées sans autorisation lors de leur transmission électronique ou lors de leur transport ou de leur conservation sur des supports de données, et qu'il est possible de vérifier

et d'établir à quels organismes des données à caractère personnel doivent être transmises par des équipements de transmission de données :
• Une transmission de données à caractère personnel effectuée pour le compte de clients ne peut avoir lieu que dans la mesure convenue avec le client ou dans la mesure nécessaire à la fourniture des prestations contractuelles au client.
• Tous les collaborateurs d'ATLAS.ti travaillant sur un projet client sont informés de l'utilisation autorisée des données et des modalités de transmission des données.
• Dans la mesure du possible, les données sont transmises aux destinataires sous forme chiffrée.
• Il est interdit aux collaborateurs d'ATLAS.ti d'utiliser des supports de stockage de données privés dans le cadre de projets clients.

b. Contrôle de la saisie
Mesures garantissant qu'il peut être vérifié et établi a posteriori si et par qui des données à caractère personnel ont été saisies, modifiées ou supprimées dans les systèmes de traitement de données :
• Journalisation de la saisie, de la modification et de la suppression de données
• Traçabilité de la saisie, de la modification et de la suppression de données au moyen de noms d'utilisateur individuels (et non de groupes d'utilisateurs)

3. Disponibilité et résilience (art. 32, paragraphe 1, point b) du RGPD)
a. Contrôle de la disponibilité
Mesures garantissant que les données à caractère personnel sont protégées contre la destruction ou la perte accidentelles :
• Alimentation électrique sans interruption (ASI)
• Dispositifs de surveillance de la température et de l'humidité dans les salles de serveurs
• Systèmes de détection d'incendie et de fumée
• Élaboration d'un concept de sauvegarde et de restauration
• Élaboration d'un plan d'urgence
• Salles de serveurs non situées sous des installations sanitaires
• Climatisation des salles de serveurs
• Blocs multiprises protégés dans les salles de serveurs
• Dispositifs d'extinction d'incendie dans les salles de serveurs
b. Capacité de restauration (art. 32, paragraphe 1, point c) du RGPD)

Mesures garantissant que les données à caractère personnel peuvent être restaurées sans délai en cas de perte ou de perturbation :
• Sauvegardes régulières
• Tests de restauration des données

4. Procédures de contrôle, d'appréciation et d'évaluation réguliers (art. 32, paragraphe 1, point d) du RGPD ; art. 25, paragraphe 1 du RGPD)
a. Gestion de la protection des données et de la sécurité de l'information
Chez ATLAS.ti, un système de gestion de la protection des données est mis en œuvre. Il existe une directive relative à la protection et à la sécurité des données ainsi que des directives visant à garantir la réalisation des objectifs de cette directive. Toutes les directives sont régulièrement évaluées et ajustées quant à leur efficacité.
Une équipe chargée de la protection des données et de la sécurité de l'information a été mise en place pour planifier, mettre en œuvre et évaluer les mesures de protection et de sécurité des données et y apporter des ajustements.
Un délégué à la protection des données a été désigné.
Tous les collaborateurs reçoivent régulièrement une formation en matière de protection des données et de sécurité de l'information.

b. Gestion de la réponse aux incidents
Tous les collaborateurs sont informés et formés afin de garantir que les incidents relatifs à la protection des données soient reconnus par l'ensemble des collaborateurs et signalés sans délai à l'équipe chargée de la protection des données et de la sécurité de l'information. Cette équipe examine l'incident immédiatement. Dans la mesure où sont concernées des données traitées pour le compte de clients, il est garanti que ceux-ci sont informés sans délai de la nature et de l'ampleur de l'incident.

c. Protection des données dès la conception et par défaut (art. 25, paragraphe 2 du RGPD)
Chez ATLAS.ti, nous veillons à ce que le principe de nécessité et de minimisation des données soit pris en compte dès le stade du développement logiciel.

d. Contrôle de la commande
Mesures garantissant que les données à caractère personnel traitées sur commande ne peuvent être traitées que conformément aux instructions du client :

• Sélection rigoureuse des sous-traitants ultérieurs (en particulier au regard de la sécurité de l'information)
• Contrôle régulier des sous-traitants ultérieurs