CONTRAT DE TRAITEMENT DE TÂCHES D'APRÈS L'ART. 28, AL. 3 DU RGPD

Donneur d'ordre (responsable) :

Prénom et nom du partenaire de coopération | Numéro du partenaire de coopération

Raison sociale

Rue, numéro | CP, localité

Fournisseur (responsable du traitement) :
ThomasLloyd Global Asset Management GmbH
Hanauer Landstraße 291b
D-60314 Francfort-sur-le-Main
Allemagne

1. Objet et durée de la convention

La mission comprend ce qui suit :
Exécution régulière d'actions de publipostage récurrentes conformément à chacune des commandes individuelles ; publipostages à des clients et personnes intéressées du responsable (les adresses seront remises par le responsable), examen des données d'adresses quant à leur aptitude à l'expédition, dédoublonnages au nom du responsable ; personnalisation des publipostages au responsable ; validation des corrections au responsable ; envoi gratuit du publipostage.

À ce sujet, le fournisseur traite des données à caractère personnel pour le donneur d'ordre, au sens de l'art. 4, n° 2 et de l'art. 28 du RGPD, sur la base du présent contrat.

Le traitement des données dans le cadre de ce traitement de tâches a généralement lieu en République fédérale d'Allemagne, dans un État membre de l'Union européenne ou dans un autre État signataire de l'Accord sur l'Espace économique européen (EEE) et en Suisse. Le fournisseur est tout de même autorisé à traiter des données à caractère personnel du donneur d'ordre dans le respect des règlements de cette convention, également en dehors de l'EEE, s'il informe le donneur d'ordre en temps utile dudit traitement et du lieu d'exécution et si les prérequis particuliers des art. 44 à 48 du RGPD sont remplis ou qu'une dérogation est constatée au sens de l'art. 49 du RGPD. La Suisse offre, d'après une décision d'adéquation de la Commission européenne, un niveau adéquat de protection des données, au sens des art. 44 ss du RGPD.

2. Durée du contrat

Le contrat commence avec la signature de la présente convention par les deux parties et prend fin par la résiliation de l'une des parties. La résiliation doit intervenir sous forme écrite et être assortie d'un préavis de 4 semaines.

Le donneur d'ordre peut résilier le contrat à tout moment sans observer de préavis dans le cas d'une violation grave de la part du fournisseur de prescriptions relatives à la protection des données ou des dispositions du présent contrat, si le fournisseur ne peut ou ne veut pas exécuter une instruction du donneur d'ordre ou si le fournisseur refuse les droits de contrôle du donneur d'ordre en des termes contraires aux dispositions du contrat. En particulier, le non-respect des obligations convenues dans le présent contrat et déduites de l'art. 28 du RGPD représente une violation grave.

3. Type et finalité du traitement, type des données à caractère personnel, ainsi que catégories des personnes concernées :

Type de traitement (conformément à la définition de l'art. 4, n° 2, du RGPD) :
- réception et sauvegarde des ensemble des coordonnées (nom, adresse, courriel) des clients et personnes intéressées à démarcher, émanant du responsable
- dédoublonnage
- envoi des publicités en lien avec l'action respective de « publipostage postal ThomasLloyd » ou de « publipostage électronique ThomasLloyd »

Type des données à caractère personnel (conformément à la définition de l'art. 4, n° 1, 13, 14 et 15 du RGPD) :
- ensemble des coordonnées (nom, adresse, courriel) des clients et personnes intéressées à démarcher, émanant du responsable

Catégories de personnes concernées (conformément à la définition de l'art. 4, n° 1 du RGPD) :
- clients ou personnes intéressées du responsable

4. Droits et obligations, ainsi que pouvoirs d'instruction du donneur d'ordre

Le donneur d'ordre est le seul responsable de l'appréciation de l'admissibilité du traitement, conformément à l'art. 6, par. 1 du RGPD, et de la préservation des droits des personnes concernées, suivant les art. 12 à 22 du RGPD. Néanmoins, le fournisseur est tenu de transmettre sans tarder toutes les demandes au donneur d'ordre, dans la mesure où elles sont manifestement adressées exclusivement à celui-ci.

Des changements de l'objet du traitement et de procédure doivent être coordonnés en commun entre le donneur d'ordre et le fournisseur et être consignés par écrit ou dans un format électronique documenté.

Le donneur d'ordre fournit tous les ordres, ordres partiels et instructions en règle générale par écrit ou dans un format électronique documenté. Des instructions orales doivent être confirmées sans tarder par écrit ou dans un format électronique documenté.

Le donneur d'ordre est habilité à juger, comme indiqué au point n° 6, avant le début du traitement et ensuite régulièrement et d'une manière appropriée, du respect des mesures techniques et organisationnelles prises auprès du fournisseur, conformément à l'annexe 1, ainsi que des obligations consignées dans le présent contrat. Le donneur d'ordre informe le fournisseur sans retard s'il constate des erreurs ou des irrégularités lors de l'examen des résultats de la mission.

Les partenaires contractuels sont tenus l'un envers l'autre de traiter de manière confidentielle toutes les connaissances de secrets commerciaux et de mesures de sécurité des données de l'autre partenaire contractuel respectif, acquises dans le cadre de la relation contractuelle. Ladite obligation persiste même après la fin du présent contrat.

5. Personnes autorisées à donner des instructions de la part du donneur d'ordre, personne destinataire des instructions de la part du fournisseur

Les personnes autorisées à donner des instructions de la part du donneur d'ordre sont :

---

prénom, nom, unité organisationnelle, téléphone

---

prénom, nom, unité organisationnelle, téléphone

La personne destinataire des instructions de la part du fournisseur est l'interlocuteur respectif du donneur d'ordre.

En cas de changement ou d'empêchement à plus long terme des interlocuteurs, il y a lieu de communiquer sans tarder et en principe par écrit ou par voie électronique au partenaire contractuel les successeurs ou les représentants. Les instructions doivent être conservées pour la durée de leur validité puis encore pendant trois années civiles complètes.

6. Obligations du fournisseur

Le fournisseur traite des données à caractère personnel exclusivement dans le cadre des conventions conclues et sur instructions du donneur d'ordre, dans la mesure où il n'est pas tenu à un autre traitement de par le Droit de l'Union ou de l'État auquel est soumis le responsable du traitement (par ex. des enquêtes d'autorités répressives ou de protection de l'État) ; dans un tel cas, le responsable du traitement informe le responsable de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public (art. 28, par. 3, phrase 2, let. a, du RGPD).

Le fournisseur utilise les données à caractère personnel qui lui ont été remises pour le traitement à aucune autre finalité, en particulier pas pour ses besoins propres. Il ne sera pas établi de copies ou de duplicatas des données à caractère personnel sans que le donneur d'ordre en ait connaissance.

Pour le traitement des données à caractère personnel conforme à la mission, le fournisseur garantit le suivi conforme au contrat de toutes les mesures convenues. Il garantit la séparation stricte des données traitées pour le donneur d'ordre d'autres bases de données

Les supports de données, qui proviennent du donneur d'ordre ou qui sont utilisés pour le donneur d'ordre, seront spécialement identifiés. L'arrivée et le départ, ainsi que l'utilisation courante, seront documentés.

Le fournisseur doit exécuter pour le donneur d'ordre en particulier les examens suivants dans son domaine, sur l'ensemble du suivi de la prestation de service :
- respect et mise en œuvre des mesures techniques et organisationnelles, consignées dans les annexes.
- Le résultat des contrôles doit être documenté.

Le fournisseur doit contribuer dans toute l'étendue nécessaire à la satisfaction des droits des personnes concernées par le donneur d'ordre suivant les art. 12 à 22 du RGPD, à l'établissement de bordereaux d'activités de traitement ainsi qu'aux études d'impact indispensables à la protection des données par le donneur d'ordre et le fournisseur doit à ce sujet soutenir le donneur d'ordre dans la mesure du possible (art. 28, par. 3, phrase 2, let. e et f du RGPD).

Le fournisseur informera immédiatement le donneur d'ordre si une instruction délivrée par le donneur d'ordre, selon lui, constitue une violation de prescriptions légales (art. 28, par. 3, phrase 3 du RGPD). Le fournisseur est habilité à interrompre l'exécution de l'instruction correspondante jusqu'à ce qu'elle soit confirmée ou modifiée après examen par le responsable du donneur d'ordre.

Le fournisseur doit corriger ou supprimer les données à caractère personnel qui ressortent de la relation contractuelle ou en limiter le traitement, si le donneur d'ordre l'exige au moyen d'une instruction et si les intérêts légitimes du fournisseur ne s'y opposent pas.

Le fournisseur n'a le droit de fournir des renseignements sur des données à caractère personnel émanant de la relation contractuelle à des tiers ou à la personne concernée que sur instruction préalable ou après approbation du donneur d'ordre.

Le fournisseur donne son accord d'habiliter le donneur d'ordre – en principe après entente sur la date – à contrôler lui-même ou à faire contrôler par des tiers, mandatés par le donneur d'ordre, le respect des prescriptions portant sur la protection et la sécurité des données ainsi que des conventions contractuelles dans la mesure appropriée et nécessaire, en particulier par l'obtention de renseignements et la consultation des données sauvegardées et des programmes de traitements de données, ainsi que par des examens et inspections sur place (art. 28, par. 3, phrase 2, let. h du RGPD).

Le fournisseur garantit de coopérer auxdits contrôles dans la mesure nécessaire.

Le traitement de données dans des domiciles privés (télétravail ou travail à domicile d'employés du fournisseur) n'est pas autorisé.

Le fournisseur confirme de connaître les prescriptions en vigueur du RGPD en termes de Droit relatif à la protection des données et qui concernent le traitement de tâches.

Le fournisseur s'engage à la confidentialité lors du traitement conforme à la mission des données à caractère personnel du donneur d'ordre. Ladite confidentialité persiste aussi après la fin du contrat.

Le fournisseur garantit de familiariser les collaborateurs, employés lors de l'exécution des tâches, avant la prise en charge de l'activité avec les dispositions, déterminantes pour eux, de la protection des données et pour le temps de leur activité, tout comme il les oblige d'une manière appropriée de respecter la confidentialité après la fin de l'emploi (art. 28, par. 3, phrase 2, let. b et art. 29 du RGPD). Au sein de son entreprise, le fournisseur surveille le respect des prescriptions en termes de Droit de protection des données.

Le responsable de la protection des données chez le fournisseur est

- **Monsieur Andreas Obrist**, ThomasLloyd Global Asset Management (Suisse) SA ; Uraniastrasse 35, CH-8001 Zurich ; courriel : gdpr@thomas-lloyd.com

Un changement du responsable de la protection des données doit être communiqué sans tarder au donneur d'ordre.

7. Obligations de communication du fournisseur en cas d'incidents dans le traitement et de violations de la protection de données à caractère personnel

Le fournisseur communique sans tarder au donneur d'ordre des incidents, des violations de la part du fournisseur ou des personnes qu'il emploie, ainsi qu'à l'encontre de dispositions en termes de Droit de protection des données ou à l'encontre des dispositions prises au cours de la mission, ainsi que la suspicion de violations de la protection des données ou d'irrégularités dans le traitement de données à caractère personnel. La règle s'applique notamment aussi à d'éventuelles obligations de notification et de communication du donneur d'ordre, suivant l'art. 33 et l'art. 34 du RGPD. Le fournisseur garantit d'assister de manière appropriée le donneur d'ordre dans ses obligations découlant des art. 33 et 34 du RGPD (art. 28, par. 3, phrase 2, let. f, du RGPD), si besoin. Le fournisseur ne peut se charger des notifications - suivant les art. 33 ou 34 du RGPD - pour le donneur d'ordre qu'après instruction préalable conformément au ch. 4 du présent contrat.

8. Relations de sous-traitance avec des sous-traitants (art. 28, par. 3, phrase 2, let. d du RGPD)

Le donneur d'ordre autorise le fournisseur de manière générale à impliquer d'autres exécutants (ci-après « sous-traitants ») dans le traitement des tâches, notamment des entreprises associées au fournisseur, par ex. ThomasLloyd Global Asset Management (Suisse) SA. Si des entreprises associées et domiciliées dans un état tiers sont impliquées, le fournisseur informe le donneur d'ordre séparément des mesures prises pour la garantie d'un niveau de protection des données adéquat d'après l'art. 44 ss du RGPD.

Le fournisseur fixera les conventions avec les sous-traitants dans un contrat écrit et rédigé de sorte que les obligations contractuelles et d'éventuelles dispositions complémentaires incombant au fournisseur s'appliquent également aux sous-traitants. Les parties conviennent que cette exigence est remplie si les accords contractuels entendus avec le sous-traitant présentent un niveau de protection correspondant à cet accord et/ou que les obligations prescrites à l'art. 28, al. 3 du RGPD s'imposent au sous-traitant.

Les prestations de service que le fournisseur attribue à des tiers comme des prestations secondaires ne s'entendent pas comme des relations de sous-traitance au sens des règlements précédemment cités. En font par exemple partie les prestations de télécommunication, de nettoyage ou, dans certaines circonstances, les prestations de contrôle ou de maintenance, même si un accès aux données à caractère personnel du donneur d'ordre ne peut être exclu. Si de telles prestations secondaires sont sous-traitées, le donneur d'ordre prendra également des dispositions adaptées pour protéger la confidentialité des données du fournisseur.

Dans le respect des exigences du point 1 de cette convention, les règlementations du point 8 s'appliquent aussi si un sous-traitant est impliqué dans un état tiers. Le donneur d'ordre déclare être disposé à participer à l'exécution des conditions particulières des art. 44 ss du RGPD.

9. Mesures techniques et organisationnelles, suivant l'art. 32 du RGPD (art. 28, par. 3, phrase 2, let. c du RGPD)

Un niveau de protection approprié au risque relatif aux droits et libertés des personnes physiques concernées par le traitement est garanti pour le traitement de tâches. Sont pris en compte à cet effet, les objectifs de protection de l'art. 32, par. 1 du RGPD, comme la confidentialité, l'intégrité et la disponibilité des systèmes et services, ainsi que leur résilience par rapport à la nature, la portée, le contexte et la finalité des traitements, de telle sorte que le risque est contenu sur la durée par le biais de mesures correctives techniques et organisationnelles appropriées.

Les mesures techniques et organisationnelles décrites dans l'annexe 1 en vue de la protection et de la sécurité des données auprès du fournisseur représentent la sélection des mesures techniques et organisationnelles qui conviennent pour le risque déterminé, en tenant compte des objectifs de protection détaillés suivant l'état de la technique et en tenant particulièrement compte des systèmes IT utilisés et des processus de traitement chez le fournisseur.

Le fournisseur doit entreprendre lorsque l'occasion en est donnée mais au moins une fois par an, un examen, une analyse et une évaluation de la validité des mesures techniques et organisationnelles suivant l'annexe 1, afin de garantir la sécurité du traitement (art. 32, par. 1, let. d du RGPD). Le résultat, y compris le rapport d'audit complet, doit être communiqué au donneur d'ordre.

S'il en résulte une nécessité de réparation ou un besoin d'adaptation des mesures techniques et organisationnelles, le fournisseur en informera le donneur d'ordre sans tarder. En outre, le fournisseur assiste le donneur d'ordre dans la documentation relative au respect des mesures techniques et organisationnelles indispensables, conformément à l'art. 32 du RGPD. Dans la mesure où un contrôle par le donneur d'ordre, effectué avant le début ou pendant le traitement de la tâche, affiche une nécessité de réparation ou un besoin d'adaptation des mesures techniques et organisationnelles ou dans la mesure où ladite nécessité ou ledit besoin s'avère indispensable pour d'autres raisons, ceux-ci seront satisfaits et documentés d'un commun accord par le fournisseur. La documentation doit être remise au donneur d'ordre ; les mesures documentées deviennent la composante et le fondement du présent contrat.

Des décisions notables, relatives à l'organisation du traitement des données et aux procédés appliqués et qui sont significatives pour la sécurité, doivent être coordonnées entre le fournisseur et le donneur d'ordre.

Dans la mesure où les mesures prises chez le fournisseur ne satisfont pas les exigences du donneur d'ordre, le donneur d’ordre en informe le fournisseur sans tarder.

Les mesures prises chez le fournisseur peuvent être adaptées à l'évolution technique et organisationnelle au cours de la relation contractuelle mais ne doivent pas se trouver en deçà des normes convenues. Le fournisseur est tenu de coordonner des changements essentiels avec le donneur d'ordre sous une forme documentée (écrite, électronique). De telles coordinations doivent être conservées pour la durée du présent contrat.

10. Obligations du fournisseur après la fin de la mission, art. 28, par. 3, phrase 2, let. g, du RGPD

À la fin de cette convention, le fournisseur doit remettre au donneur d'ordre tou(te)s les données, documents et résultats établis du traitement ou de l'utilisation qui se trouvent en sa possession et qui sont en rapport avec la relation contractuelle ou les effacer à sa demande, conformément aux règles inhérentes à la protection des données ou les détruire / faire détruire.

L'effacement, voire la destruction, doit être confirmée au donneur d'ordre avec indication de la date, par écrit ou dans un format électronique documenté.

11. Responsabilité

Il est fait référence à l'art. 82, art. 1 du RGPD. Par ailleurs, il est convenu ce qui suit :
Si tant le donneur d'ordre que le fournisseur sont responsables d'un dommage conformément à l'art. 82, par. 2 du RGPD, les partenaires contractuels sont responsables en interne pour ledit dommage, proportionnellement à leur part de responsabilité. Si, dans un tel cas, une personne réclame une indemnisation à un partenaire contractuel en totalité ou au-dessus de de la part de responsabilité du partenaire contractuel concerné, ledit partenaire contractuel peut exiger de l'autre partenaire contractuel l'exemption ou le dédommagement, dans la mesure où l'indemnisation va au-delà de sa part de responsabilité.

12. Autres dispositions

Des conventions relatives aux mesures techniques et organisationnelles ainsi que des documents de contrôle et d'audit doivent être conservés par les deux partenaires contractuels pour la durée de leur validité puis pour trois années civiles complètes au-delà. Des conventions annexes nécessitent la forme écrite ou un format électronique documenté.

Si la propriété ou les données à caractère personnel à traiter du donneur d'ordre sont menacées chez le fournisseur par des mesures de tiers (comme par exemple une saisie ou une confiscation), par une procédure de faillite ou de concordat ou par d'autres évènements, le fournisseur doit en avertir le donneur d'ordre sans tarder.

L'exception du droit de rétention dans le sens de l'§ 273 du Code civil allemand est exclue eu égard aux données traitées pour le donneur d'ordre et aux supports de données associés.

Si des parties spécifiques de la présente convention s'avéraient non valides, ceci n'affecterait pas par ailleurs la validité de la convention.

Signatures :

_____ _____

Donneur d'ordre Fournisseur

Annexe 1 : Description des mesures techniques et organisationnelles relatives à la protection et à la sécurité des données chez ThomasLloyd

ANNEXE 1
AU CONTRAT DE TRAITEMENT DE TÂCHES, SUIVANT L'ART. 28, PAR. 3 DU RGPD

Description des mesures techniques et organisationnelles relatives à la protection et à la sécurité des données chez ThomasLloyd

Suivant l'art. 28, par. 3 du RGPD, les mesures techniques et organisationnelles à prendre suivant l'art. 32 du RGPD, doivent être consignées par écrit.

La mise en œuvre et le respect des mesures techniques et organisationnelles suivantes seront examinés par le biais de contrôles réguliers du responsable de la protection des données chez ThomasLloyd.

1. Contrôle d'entrée

Mesures qui interdisent à des personnes non autorisées l'accès à des documents de traitement de données et avec lesquelles des données à caractère personnel sont traitées ou utilisées :
- la porte d'entrée au bureau est fermée en permanence (pendant et en-dehors des heures d'ouverture) ;
- il existe un contrôle d'accès électronique s'appuyant sur une puce, avec établissementd'un journal ;
- l'attribution des puces et des clés est documentée ;
- la zone d'entrée se trouve dans le champ visuel du personnel du secrétariat et de la réception ;
- les personnes extérieures ne doivent, ni ne peuvent se déplacer qu'en étant en permanence accompagnées dans le bureau ;
- les visiteurs seront inscrits dans un livre des visiteurs ;
- l'installation d'alarme en dehors des heures de bureau est active ; il existe un blocage supplémentaire du verrouillage électronique de l'entrée, fondé sur une puce ;
- accès aux locaux techniques du serveur et du réseau réservé aux responsables IT et à leurs adjoints.

2. Contrôle d'utilisation

Mesures destinées à empêcher des personnes non autorisées d'utiliser les systèmes de traitement des données :
- tous les systèmes TD ne sont utilisables qu'avec nom d'utilisateur et mot de passe ;
- nom d'utilisateur et mot de passe sont attribués individuellement ;
- les mots de passe sont confidentiels et doivent impérativement posséder une longueur minimale ;
- les mots de passe doivent impérativement être changés régulièrement ;
- le même mot de passe ne peut être utilisé plusieurs fois ;
- blocage du poste de travail après 20 minutes d'inactivité ; le blocage ne peut être supprimé que par le biais de l'utilisateur inscrit ou de l'administrateur ;
- les systèmes des serveurs ne peuvent être administrés qu'à la console ou par l'intermédiaire d'une liaison cryptée ;
- les systèmes des serveurs sont protégés par des mots de passe différents ;
- l'accès aux données et processus des systèmes des serveurs n'est possible que dans les limites du réseau interne ; il n'existe pas de client externe ; fermeture vers l'extérieur par concept de pare-feu en deux phases, y compris système de détection d'intrusion (SDI), avec logiciels de fabricants différents ;
- double scannage de virus par logiciels de fabricants différents, avec actualisation au moins quotidienne des signatures ;
- il existe un scan complet des virus, à base de règles.

3. Contrôle d'usage

Mesures destinées à garantir que les personnes, habilitées à utiliser un système de traitement de données, peuvent accéder exclusivement aux données soumises à leur habilitation d'accès et que les données à caractère personnel ne pourront pas être lues, copiées, modifiées ou supprimées de manière non autorisée lors du traitement, de l'utilisation et après la sauvegarde :
- création de comptes de collaborateurs personnalisés ;
- attribution d'habilitations d'accès réservée aux collaborateurs directement impliqués exclusivement aux données qui s'avèrent nécessaires pour les tâches à accomplir (système de droit d'accès à base de rôle) ;
- l'attribution de droits est assurée de manière centralisée par l'administrateur du système, séparément pour les fonctions de la consultation de fichiers, de la création, l'écriture, la modification, l'effacement, la lecture et la commande de l'accès ;

- les droits d'accès seront attribués suivant les directives relatives aux groupes, dans des cas exceptionnels de façon individuelle ;
- les droits peuvent être attribués au dernier moment puis à nouveau être retirés ;
- examen des droits d'accès lors de chaque authentification vis-à-vis des postes de travail et des serveurs ;
- décision de validation n'appartenant qu'à la Direction ou aux responsables de la zone de données ;
- enregistrement des habilitations d'accès dans un journal ;
- identification claire des ordinateurs par le serveur, par l'intermédiaire d'examen de l'adresse IP ;
- protection des postes de travail contre des modifications non autorisées du matériel ou du logiciel ;
- protection, sans cesse actualisée, des postes de travail et des serveurs contre des attaques de virus et des logiciels malveillants ;
- fermeture du réseau interne par un système de pare-feu et de détection d'intrusion à plusieurs niveaux, entretenu et surveillé en permanence ;
- accès limité à l'Internet (basé sur des règles).

4. Contrôle de diffusion

Mesures destinées à garantir que des données à caractère personnel ne peuvent être lues, copiées, modifiées ou supprimées de manière non autorisée lors de la transmission électronique ou pendant leur transport ou leur sauvegarde sur des supports de données et qu on puisse vérifier et constater à quels endroits est prévue une transmission de données à caractère personnel par des dispositifs visant la transmission de données :

- la transmission électronique de données a lieu conformément aux conventions concrètes, conclues avec des destinataires autorisés ;
- les données à caractère personnel sont transmises de préférence par l'intermédiaire d'un serveur Internet, sécurisé par SSL (« coffre-fort pour documents ») (https, hautement crypté, RSA 2048 bits, signé Verisign) ;
- l'accès au coffre-fort pour documents n'est possible que par l'intermédiaire de comptes personalisés ;
- les données ne sont pas sauvegardées sur les postes de travail ;
- les données sont sauvegardées exclusivement par l'intermédiaire du réseau interne sur des supports de données sécurisés (serveurs) dans la salle informatique ;
- aucune donnée à caractère personnel n'est sauvegardée sur des supports de données mobiles (disquettes, CD, clés USB, etc.) ;
- néanmoins, d'autres données (par ex. des présentations) ne sont sauvegardées que par des collaborateurs autorisés sur des supports de données mobiles (disquettes, CD, clés USB, etc.) ;
- les supports de données mobiles réinscriptibles (clés USB) sont remis après leur utilisation dans le service Graphiques et les données qui s'y trouvent, supprimées ;
- après leur utilisation, des supports de données mobiles seront détruits par un prestataire de services certifié externe (documentus GmbH Berlin & Co. Betriebs KG) ;
- interdiction d'utiliser ses propres ordinateurs portables, clés USB, disques durs dans le réseau de l'entreprise ;
- blocage d'interfaces correspondantes sur les postes de travail (par ex. contrôleurs USB, unités de disquettes, disques optiques) ;
- utilisation d'interfaces correspondantes réservée à des postes de travail sélectionnés et contrôlés ;
- surveillance permanente et établissement de journaux pour les accès et processus sur tous les serveurs et dispositifs de réseaux (pare-feux, routeurs), utilisés chez le fournisseur pour la transmission électronique des données ;
- conservation des bandes de sauvegarde dans le coffre-fort ignifuge, accès uniquement par le biais du service IT ;
- la transmission de données entre les sites a lieu par VPN.

5. Contrôle de saisie

Mesures destinées à garantir qu'il peut être vérifié et constaté ultérieurement si – et par qui – des données à caractère personnel ont été intégrées, modifiées ou supprimées dans des systèmes de traitement de données:

- établissement automatique de journaux d'activités de connexion et d'activités de systèmes sur tous les postes de travail et tous les serveurs ;
- pas d'accès à des ensembles complets de données ou à plus d'un ensemble de données en même temps, pendant la collecte ou la saisie des données ;
- informations compréhensives sur les dates et les utilisateurs pour tous les fichiers ;
- établissement automatique de journaux sur tous les changements intervenus dans le système de collecte de données avec date et utilisateur ;

- sauvegarde quotidienne de toutes les données et journaux, avec informations correspondantes sur la création, le changement ou l'effacement de données ;
- conservation des supports de données de sauvegarde dans le coffre-fort.

6. Contrôle des tâches

Mesures destinées à garantir que des données à caractère personnel, qui ont été traitées au cours de la mission, ne sont traitées que conformément aux instructions du donneur d'ordre :
- la limitation des responsabilités entre donneur d'ordre et fournisseur est réglementée, en termes de mission, par le contrat respectif ;
- les interlocuteurs ThomasLloyd (« chefs de projet »), nommés dans le contrat respectif, objet de la mission, sont autorisés à instruire d'autres collaborateurs ThomasLloyd quant à l'utilisation et au traitement des données à caractère personnel ;
- instruction et obligation contractuelle de tous les collaborateurs travaillant pour ThomasLloyd par rapport au respect des dispositions relatives à la protection des données ;
- externalisation d'activités de traitement de données uniquement avec l'assentiment préalable du donneur d'ordre respectif, dans la mesure où des données du donneur d'ordre sont concernées (ce qui est exclu ici) ; conclusion de contrats de traitement de tâches ;
- coordination du questionnaire avec le donneur d'ordre et validation par celui-ci ;
- programmation conformément au questionnaire validé ;
- contrôle aléatoire de la concordance par le chef de projet et le / la responsable de la protection des données.

7. Contrôle de disponibilité

Mesures destinées à garantir la protection des données à caractère personnel contre la destruction ou la perte accidentelle :
- protection contre des virus et des logiciels malveillants, ainsi que contre la fermeture des réseaux ;
- protection de tous les postes de travail et tous les serveurs contre des défaillances ;
- systèmes de disques résistants aux pannes (RAID) ;
- duplication synchrone sur systèmes de secours ;
- garantie de reconstitution rapide, y compris des profils utilisateurs ;
- sauvegarde complète quotidienne de toutes les bases de données et de toute la communication par courriel ;
- copie quotidienne de sécurité pour tous les serveurs importants, y compris les réglages du système et l'établissement de journaux ;
- stockage protégé contre les vols, l'emploi abusif et l'incendie, des supports de données de sécurité dans le coffre-fort, à l'intérieur du bureau et à l'extérieur (autre partie du bâtiment) ;
- existence de mise en mémoire tampon ASI ;
- fermeture vers l'extérieur par concept de pare-feu en deux phases, y compris système de détection d'intrusion (SDI), avec logiciels émanant de fabricants différents ;
- double scannage de virus par logiciels émanant de fabricants différents, avec actualisation quotidienne multiple des signatures.

8. Principe de séparation

Mesures destinées à garantir que des données prélevées à des fins différentes seront traitées séparément :
- séparation des clients, conforme à la protection des données, suivant les donneurs d'ordre et les tâches ;
- séparation organisationnelle entre la mise au point et la réalisation des programmes, la collecte et le traitement des données, ainsi que les autres secteurs de l'entreprise ;
- présentation du contrôle organisationnel en directives de groupes et droits d'accès ;
- conservation physiquement séparée de données de consultation et de données à caractère personnel ;
- accès conformément au concept d'habilitation ;
- effacement de données à caractère personnel à la fin de la mission, conformément aux prescriptions des donneurs d'ordre respectifs.