Contrat de sous-traitance entre

Karl Wörwag Lack- und Farbenfabrik GmbH & Co. KG
Strohgäustraße 28, 70435 Stuttgart

et

FOURNISSEURS

Préambule

Les parties contractantes ont, par le biais du contrat de service, conclu un contrat de sous-traitance, et ce conformément à l'article 28 du règlement général sur la protection des données (RGPD) de l'Union européenne ou le traitement des données stipulé dans le contrat de service effectué au nom du responsable (appelé sous-traitance). Afin de concrétiser les droits et les obligations découlant du contrat de sous-traitance conformément à l'obligation légale, les parties contractantes concluent le contrat ci-après.

1 Champ d'application

L'accord s'applique à toutes les activités qui font l'objet du contrat de service et dans le cadre desquelles les collaborateurs du sous-traitant ou des tiers mandatés par le sous-traitant entrent en contact conformément au présent accord pour le traitement de données à caractère personnel, et relevant de la compétence du responsable (article 4, alinéa 7 du RGPD).

2 Définition des termes

2.1 Le présent accord porte uniquement sur le traitement de données à caractère personnel conformément aux instructions données par le responsable.

2.2 Le traitement désigne toute opération réalisée à l'aide d'une procédure automatisée ou non ou toute série d'opérations en lien avec des données à caractère personnel, comme par exemple la collecte, la saisie, l'organisation, le classement, la sauvegarde, l'adaptation ou la modification, la lecture, la consultation, l'utilisation et la publication moyennant la transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou la mise en relation, la limitation, la suppression ou la destruction.

2.3 Les données à caractère personnel désignent toutes les informations qui portent sur une personne physique identifiée ou identifiable (ci-après désignée par la « personne concernée ») ; est considérée comme identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment à l'aide de l'attribution d'un identifiant comme par exemple un nom, un numéro d'identification,

les données de localisation, une identification en ligne ou une ou plusieurs caractéristique particulières, l'expression de l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale de cette personne physique.

2.4 Le sous-traitant est une personne physique ou morale, une autorité, un établissement ou autre organisme qui traite les données à caractère personnel sur ordre du responsable.

2.5 L'instruction est l'ordre donné par le responsable portant sur un traitement des données à caractère personnel en conformité avec la protection des données (p. ex. anonymisation, blocage, suppression, publication) du sous-traitant. Par la suite, les instructions existantes peuvent être modifiées, complétées ou remplacées (instruction individuelle) par le responsable (p. ex. moyennant un complément au contrat).

3 Concrétisation du contenu du mandat

3.1 L'objet et la durée de la sous-traitance ainsi que l'étendue, la nature et la finalité du traitement prévu des données sont stipulés dans le contrat de service.

3.2 La nature des données à caractère personnel utilisées sont décrites précisément à **l'annexe 2** (« Concrétisation des catégories de données »).

3.3 La catégorie de personnes concernées par le traitement des données à caractère personnel est décrite précisément à **l'annexe 3** (« Sous-traitants autorisés »).

4 Responsabilité et pouvoir de donner une instruction

4.1 Il incombe au responsable d'observer les dispositions de la loi sur la protection des données, notamment concernant la légalité de la transmission des données au sous-traitant ainsi que la légalité du traitement des données (article 4, alinéa 7 du RGPD). Il peut à tout moment demander la publication, la rectification, la suppression et le blocage des données (article 28, alinéa 3, lettre g) du RGPD) sauf s'il existe une obligation légale de sauvegarde des données à caractère personnel. Si une personne concernée s'adresse directement au sous-traitant à des fins de suppression ou de rectification de ses données, dans ce cas le sous-traitant transmettra directement cette demande au responsable et fournira son assistance dans le cadre de l'exécution à l'aide des informations mises à la disposition du sous-traitant (article 28, alinéa 3, lettre f) du RGPD)

4.2 Le sous-traitant est autorisé à traiter les données exclusivement dans le cadre des instructions documentées du responsable dans la mesure où il n'y est pas tenu en vertu du droit de l'Union européenne ou des États membres auquel est soumis le sous-traitant. Dans ce cas, le sous-traitant informe immédiatement le responsable de ces exigences légales avant le traitement. Une instruction est un ordre écrit du responsable visant un traitement particulier par le sous-traitant des données à caractère personnel. Les instructions sont en premier lieu définies par le contrat de prestation et peuvent ultérieurement être modifiées, complétées ou remplacées par le responsable par écrit moyennant une instruction individuelle (article 28, alinéa 3, lettre a) du RGPD).

4.3 Le sous-traitant est tenu d'informer immédiatement le responsable conformément à l'article 28, alinéa 3 du RGPD s'il estime qu'une instruction viole les dispositions prescrites par la loi sur la protection des données. Le sous-traitant a le droit de différer l'exécution de l'instruction correspondante tant qu'elle n'est pas confirmée ou modifiée par le responsable.

4.4 Toute modification de l'objet du traitement, accompagnée d'un changement de procédure, doit être convenue d'un commun accord et documentée. Le sous-traitant n'est autorisé à donner des renseignements aux tiers ou personnes concernées que sous réserve du consentement écrit préalable du responsable. Le sous-traitant utilise utile les données à aucune autre fin et notamment il lui est interdit de les transmettre à un tiers. Il est interdit de faire des copies et duplicatas à l'insu du responsable. Il en va autrement uniquement s'il existe une disposition y afférente dans le contrat ou dans les cas stipulés au paragraphe 4.2 du présent accord.

4.5 Le responsable tient le registre des activités de traitement conformément à l'article 30, alinéa 1 du RGPD. Le sous-traitant met à la disposition du responsable, à la demande de celui-ci, les informations sur l'inscription au registre des acticités de traitement.

4.6 Le traitement et l'utilisation des données sur ordre du responsable a lieu exclusivement au sein de l'Union européenne ou dans l'Espace économique européen. Un transfert vers un État en dehors du territoire national de la République fédérale d'Allemagne nécessite le consentement préalable du responsable. Cette disposition ne s'applique pas aux entreprises liées au sous-traitant conformément à l'article 15 de la loi allemande sur les sociétés anonymes *(Aktiengesetz)* dans la mesure où des règles d'entreprise contraignantes ou des clauses contractuelles types ont été conclues avec ces entreprises. Il n'est pas dérogé aux conditions préalables particulières des articles 44 à 49 du RGPD pour les autres cas.

4.7 Un traitement des données à caractère personnel au domicile des collaborateurs du sous-traitant (télétravail, postes de travail à domicile) n'est autorisé que sous réserve des conditions préalables suivantes : il s'agit du matériel du sous-traitant qui a été confié aux collaborateurs à des fins professionnelles, protégé par un pare-feu et sécurisé par un certificat client VPN (réseau privé virtuel). Les accès du matériel privé des collaborateurs ne sont en aucun cas autorisés.

5 Observation responsable des obligations légales contraignantes par le sous-traitant

5.1 Outre les dispositions contractuelles du présent accord et du contrat de service, le sous-traitant honore les obligations légales ci-dessous conformément à l'article 28, alinéa 3 et l'article 30 du RGPD.

5.2 Le sous-traitant garantit que les collaborateurs chargés du traitement des données du responsable sont tenus par une obligation conformément à l'article 5, lettre c) du RGPD et qu'ils ont été informés des dispositions de protection de la loi sur la protection des données. Cela comprend également l'information sur le lien existant avec l'instruction et la finalité dans le présent contrat de sous-traitance.

5.3 Le sous-traitant a désigné un responsable opérationnel de la protection des données conformément à l'article 37 du RGPD, qui exerce son activité conformément aux articles 38 et 39 du RDPG. Les coordonnées du responsable de la protection des données doivent être communiquées au responsable à des fins de prise de contact directe.

5.4 Le sous-traitant informe le responsable sans délai des contrôles et des mesures qui sont fixées par les autorités de surveillance conformément à l'article 58 du RGPD ou qu'une autorité de surveillance impose au sous-traitant conformément à l'article 83 du RGPD. Par ailleurs, le sous-traitant informe immédiatement le responsable s'il est poursuivi en justice et visé par une action en dommages-intérêts en raison d'une violation du RPGD et puis il l'informe régulièrement de la procédure en instance.

5.5 Le sous-traitant s'engage, au moment de l'entrée en vigueur du RGPD, à tenir un registre des activités de traitement, lequel contient toutes les catégories d'activités de traitement réalisées sur ordre (article 30, alinéa 2 du RGPD). Ce registre contient au minimum :

(a) le nom et les coordonnées du sous-traitant et de chaque collaborateur du responsable, pour le compte duquel le sous-traitant exerce son activité, ainsi que le cas échéant du représentant du responsable ou du sous-traitant et d'un éventuel responsable de la protection des données ;

(b) les catégories de traitement qui sont réalisées sur ordre du responsable ;

(c) le cas échéant les transmissions de données à caractère personnel à un pays tiers ou à une organisation internationale, y compris l'indication du pays tiers concerné ou de l'organisation internationale concernée, ainsi que la documentation de garanties adéquates dans le cadre des transmissions de données visées par l'article 49, alinéa 1, tiret 2 ;

(d) si possible, une description générale des mesures techniques et organisationnelles conformément à l'article 32, alinéa 1 du RGPD.

Le sous-traitant accorde au responsable, sur demande et dans un délai de 14 jours suivant la demande écrite, la consultation des informations du registre concernées par ce traitement.

6 Sécurité du traitement et contrôle y afférent

6.1 Les parties contractantes conviennent des mesures de sécurité sur le plan technique et organisationnel consignées de façon concrète à **l'annexe 1** « Mesures techniques et organisationnelles » du présent accord, et ce conformément à l'article 28, alinéa 3, lettre c) du RGPD en lien avec l'article 32, alinéa 1 du RGPD ou l'article 22 BDSG 2018 afin de garantir la sécurité du traitement. L'annexe fait l'objet du présent accord.

6.2 Les mesures techniques et organisationnelles tiennent compte au moment de la conclusion du présent accord de l'état actuel de la technique et sont soumises aux progrès de la technologie. Le sous-traitant est ainsi autorisé à mettre en œuvre des mesures alternatives adéquates. Pour ce faire, les mesures en question ne doivent pas se situer en-deçà de celles qui sont définies à **l'annexe 1** « Mesures techniques et organisationnelles ». Les modifications essentielles doivent être documentées.

6.3 Le sous-traitant s'engage à vérifier et à évaluer l'efficacité des mesures techniques et organisationnelles concrètes en ce qui concerne la sécurité du traitement, et à documenter l'évaluation des risques.

6.4 Le sous-traitant donnera au responsable, sur demande, les renseignements nécessaires pour garantir son obligation de contrôler le mandat et mettra à disposition les preuves correspondantes. Compte tenu de l'obligation de contrôle du responsable conformément à l'article 28, alinéas 1 et 3 du RGPD, le sous-traitant garantit avant le début du traitement des données et pendant la durée de validité du mandat qu'il peut assurer le responsable du respect des mesures techniques et organisationnelles prises. Pour ce faire, le sous-traitant prouve au responsable, sur demande, la mise en œuvre des mesures techniques et organisationnelles conformément à l'article 32, alinéa 1 ainsi que la réalisation de l'évaluation des risques effectuée régulièrement conformément au paragraphe 6.3. La preuve de la mise en œuvre desdites mesures qui concernent non seulement le mandat concret mais peut aussi être fournie sur présentation d'une attestation actuelle ou de rapports émanant d'instances indépendantes (p. ex. expert-comptable, audit, responsable de la protection des données, département de la sécurité informatique, auditeurs en matière de protection des données) ou une propre certification par le biais d'un audit sur la sécurité informatique ou la protection des données (p. ex. protection de base selon BSI, ISO 27001).

6.5 Le responsable, pour forger sa propre conviction, peut se rendre dans les unités de production du sous-traitant, aux heures normales d'ouverture, sans gêner le déroulement des opérations, à des fins

de vérification de l'adéquation des mesures visant à répondre aux exigences techniques et organisationnelles des lois sur la protection des données applicables à la sous-traitance (article 28, alinéa 3, lettre h) du RGPD).

7 Notification en cas de violations imputables au sous-traitant

7.1 Le sous-traitant informe le responsable sans délai après avoir constaté des perturbations graves du déroulement de ses opérations, en cas de soupçon de violations des dispositions contractuelles ou légales en matière de protection des données, en cas de violations de ces dispositions ou autres irrégularités lors du traitement des données du responsable (article 28, alinéa 3, phrase 3, articles 33 et 34 du RGPD). Pour ce faire, la notification doit contenir au minimum ce qui suit :

(a) une description du type de violation de la protection des données à caractère personnel, si possible en précisant les catégories et le nombre approximatif de personnes concernées, les catégories concernées et le nombre approximatif de fichiers de données à caractère personnel concernés ;

(b) une description des conséquences probables de la violation de la protection des données à caractère personnel ;

(c) une description des mesures déjà prises ou proposées pour remédier à la violation de la protection des données à caractère personnel et le cas échéant les mesures visant à atténuer leurs répercussions négatives éventuelles.

Si toutes les informations indiquées au paragraphe7.1, lettres a) à c) ne peuvent être mises à disposition au moment de la notification, dans ce cas lesdites informations doivent être fournies sans délai dès qu'elles sont disponibles ou mises à disposition progressivement, le cas échéant.

7.2 Le sous-traitant, dans le cadre de sa conduite à l'égard du responsable, doit prendre les mesures adéquates pour garantir la sécurité des données et pour atténuer les éventuelles conséquences négatives à l'égard des personnes concernées.

8 Suppression et restitution des données

8.1 Les supports et les fichiers de données remis demeurent la propriété du responsable.

8.2 À la demande du responsable, toutefois au plus tard à la prescription des droits découlant du contrat de service sous-jacent, le sous-traitant doit remettre au responsable tous les documents en sa possession, les résultats des traitements et utilisations ainsi que les volumes de données (y compris les copies ou les reproductions y afférentes) qui sont en rapport avec la sous-traitance ou les détruire conformément à la protection des données et sous réserve du consentement préalable du responsable (article 28, alinéa 3, lettre g) du RGPD). La même disposition s'applique au matériel de test et de rebus. Une documentation sur la garantie d'une suppression en bonne et due forme et un procès-verbal de suppression doivent être présentés au responsable, à sa demande.

8.3 Le sous-traitant peut conserver les documentations destinées à prouver le traitement des données en bonne et due forme et conformément au mandat, y compris à la fin du contrat et ce conformément aux délais de prescription ou de conservation. Autrement, il peut, à sa décharge, les remettre au responsable à la fin du contrat.

9 Sous-traitant

9.1 Le sous-traitant ne mandate aucun autre sous-traitant sans le consentement écrit préalable et particulier du responsable, et il s'engage à recourir uniquement à des sous-traitants en remplissant les conditions préalables ci-après :

(a) Le sous-traitant sélectionne le sous-traitant de façon méticuleuse et vérifie avant le mandat que ce dernier peut respecter les accords conclus entre le responsable et le sous-traitant. Notamment, le sous-traitant doit contrôler au préalable et régulièrement pendant la durée du contrat que le sous-traitant a pris les mesures techniques et organisationnelles appropriées aux fins de protection des données à caractère personnel conformément à l'article 32, alinéa 1 du RGPD. Le résultat du contrôle doit être documenté par le sous-traitant. Le sous-traitant s'engage à faire confirmer par le sous-traitant que ce dernier, si la loi l'exige, a désigné un responsable de la protection des données au sens de l'article 37 du RGPD.

(b) Le sous-traitant organise les accords contractuels avec le ou les sous-traitants de sorte qu'ils correspondent aux dispositions relatives à la protection des données dans le rapport contractuel entre le responsable et le sous-traitant.

9.2 Ne doivent pas être considérés comme des sous-traitants au sens de cette disposition les prestations de services que le sous-traitant utilise auprès de tiers à titre de prestation annexe pour le soutenir dans le cadre de l'exécution du mandat. Parmi eux figurent p. ex. les prestations de télécommunication, la maintenance et le service utilisateur, le personnel de nettoyage, l'auditeur ou l'élimination de supports de données. Le sous-traitant s'engage toutefois à garantir la protection et la sécurité des données du responsable y compris dans les prestations annexes sous-traitées, à conclure des accords contractuels adéquats et licites et à prendre des mesures de contrôle.

9.3 Au moment de la signature du contrat, les sous-traitants mandatés sont documentés à **l'annexe 3** (« Sous-traitants autorisés ») y compris les sites de traitement et le type de prestation. Les sous-traitants figurant sur cette liste sont considérés d'emblée comme mandatés de manière licite au sens du paragraphe 9, alinéa 1, dans la mesure où la mise en application des conditions préalables qui y sont stipulées est garantie par le sous-traitant.

9.4 Le sous-traitant ne peut avoir accès aux données que lorsque le sous-traitant honore les obligations du sous-traitant découlant du présent contrat ou en a fait la promesse à l'égard du sous-traitant, et le sous-traitant vérifie régulièrement le respect de ces obligations incombant au sous-traitant.

10 Prestations annexes

Les paragraphes 1 à 8 s'appliquent en conséquence lorsque le contrôle et la maintenance des procédures automatisées ou des installations de traitement des données sont effectués sur ordre d'autres organismes et ainsi un accès aux données à caractère personnel ne peut être exclu.

11 Confidentialité et contrôle de la protection des données

11.1Le responsable et le sous-traitant s'engagent à respecter la confidentialité de tous les secrets d'exploitation et commerciaux portés à leur connaissance dans le cadre du rapport contractuel. Cette disposition s'applique pendant la durée convenue dans le contrat de service, y compris au-delà de l'expiration des différents mandats ou de la relation commerciale.

11.2Le sous-traitant s'engage à accorder à tout moment un accès au responsable opérationnel de la protection des données du responsable aux heures normales d'ouverture pour exécuter ses obligations légales dans le cadre du présent mandat.

12 Dispositions finales

12.1Les modifications et les compléments à cette annexe et à toutes ses parties constitutives – y compris les éventuelles garanties du sous-traitant – nécessitent un accord écrit et la stipulation expresse selon laquelle s'il s'agit d'une modification ou d'un complément auxdites conditions. Cette disposition s'applique également à la renonciation à l'exigence de la forme écrite. La nécessité de la forme écrite ne s'applique pas si cette dernière est abrogée par les parties contractantes sur la base d'un accord explicite et individuel.

12.2Les annexes ci-après font partie intégrante du présent accord :

Annexe 1 « Mesures techniques et organisationnelles »

Annexe 2 « Concrétisation des types et catégories de données »

Annexe 3 « Sous-traitants autorisés »

Annexe 1 du contrat de sous-traitance

A. Mesures techniques et organisationnelles conformément à l'article 32, alinéa 1, lettres a) à d) du RGPD de l'UE

1. Établissement d'un pseudonyme (article 32, alinéa 1, lettre a) du RGPD de l'UE)
Les données qui doivent être évaluées uniquement à des fins statistiques font l'établissement d'un pseudonyme et sont sauvegardées sans référence à la personne. Les données qui doivent être transmises à un sous-traitant font, dans la mesure du possible, l'objet de l'établissement d'un pseudonyme et ne constituent pas ensuite des données à caractère personnel pour le sous-traitant conformément au jugement de la Cour de justice de l'UE du 19/10/16 (C 582/2014).

2. Cryptage (article 32, alinéa 1, lettre a) du RGPD de l'UE)
Les données à caractère personnel sont sauvegardées uniquement de manière cryptée sur les supports de données mobiles et les appareils portables. Un accès aux données sauvegardées dans le centre informatique n'est possible qu'avec des connexions cryptées. Les données sont transmises exclusivement de manière cryptée conformément à la directive BSI TR-2102.

3. Garantie de la confidentialité (article 32, alinéa 1, lettre b) du RGPD de l'UE)

L’intrusion de personnes non autorisées dans les systèmes de traitement des données doit être empêchée. Les habilitations sont gérées sur la base d’un concept juridique par rotation. Chaque collaborateur dispose de son accès personnel au traitement des données, protégé par un mot de passe. Le mot de passe doit obligatoirement comprendre un mélange de chiffres, de lettres de l’alphabet et de symboles et comporter huit caractères au minimum. Les différents systèmes de traitement des données doivent être verrouillés pendant les pauses. Le verrouillage ne peut être débloqué qu’à l’aide d’un mot de passe. La mise à jour des habilitations doit être régulièrement vérifiée. De nombreuses mesures garantissent que les données à caractère personnel collectées à des fins différentes peuvent être traitées séparément (par exemple, via la capacité multi-clients et le concept d'autorisation). L'accès aux salles de traitement des données est contrôlé et refusé aux personnes non autorisées. Les bureaux sont sécurisés par un système de verrouillage, les visiteurs doivent s'inscrire avec les heures de présence dans une liste. Les salles du centre de données sont sécurisées par un système d’accès électronique avec autorisations documentées; le séjour de personnes non autorisées dans le centre de données n’est autorisé que dans les cas d’entretien et uniquement en compagnie d’une personne autorisée. Les heures de présence dans le centre de données sont enregistrées électroniquement. Les processeurs ne sont chargés du traitement des données à caractère personnel que si des mesures techniques et organisationnelles équivalentes sont garanties. Les données personnelles sont, dans la mesure où il ne s'agit pas d'un processeur, uniquement transmises sur instructions de la personne responsable ou sur une base légale.

4. Garantie de l’intégrité (article 32, alinéa 1, lettre b) du RGPD de l’UE)
Seules des habilitations d’écriture limitées sont accordées en ce qui concerne les données, et des contrôles d’intégrité sont régulièrement effectués. Des contrôles de sécurité sont régulièrement entrepris, comme p.ex. des tests d’intrusion.

5. Garantie de la disponibilité (article 32, alinéa 1, lettre b) du RGPD de l’UE)
Les données doivent être protégées contre une destruction ou une perte accidentelle. En principe, toutes les données sont sauvegardées de manière redondante (au minimum via des systèmes RAID de niveau 5 ou 6 sécurisés contre les défaillances). Plusieurs sauvegardes de données redondantes et/ou répliques sont établies et stockées en dehors du bâtiment des données d’origine. Pour garantir la disponibilité, il existe une alimentation électrique sans coupure, un pare-feu et une protection contre les virus mise à jour.

6. Garantie de la capacité des systèmes (article 32, alinéa 1, lettre b) du RGPD de l’UE)
La capacité des liaisons de communication et de la capacité informatique est garantie par la surveillance continue de la charge.

7. Procédure pour restaurer la disponibilité des données à caractère personnel après un incident physique ou technique (article 32, alinéa 1, lettre c) du RGPD de l'UE)
Des tests sont régulièrement effectués pour garantir la récupération des données sauvegardées à l'aide d'une sauvegarde redondante sur différents sites et en réduisant au minimum les indisponibilités.

8. Procédure de contrôle et d'évaluation réguliers de l'efficacité des mesures techniques et organisationnelles (article 32, alinéa 1, lettre d) du RGPD de l'UE)
Il existe un concept de sécurité informatique et de protection des données dont la nécessité d'adaptation est constamment contrôlée. Les modifications sont documentées et leur efficacité est régulièrement vérifiée.

B. Mesures techniques et organisationnelles supplémentaires en cas de traitement de données sensibles conformément à l'article 22, alinéa 2 BDSG 2018 :

Les collaborateurs sont régulièrement informés de l'état actuel de la technique en matière de protection des données. Un responsable de la protection des données est désigné.

Sous réserve de l'état actuel de la technique, des frais de mise en œuvre, de la nature, de l'étendue, des circonstances et des finalités du traitement ainsi que la probabilité de la survenance et la gravité des risques liés au traitement pour les droits et les libertés des personnes physiques, les mesures de sécurité supplémentaires ci-dessous sont mises en œuvre lors du traitement de données sensibles dans le cadre de la proportionnalité et conformément à l'article 9, alinéa 1 du RGPD de l'UE :

S1. Contrôle de la saisie (article 22, alinéa 2, n° 2 BDSG 2018)

La saisie, la modification et la suppression des données à caractère personnel sensibles sont enregistrées avec mention de l'identifiant de la personne chargée du traitement qui peut être individualisé.

S2. Limitation de l'accès aux données à caractère personnel (article 22, alinéa 2, n° 5 BDSG 2018)

Les données à caractère personnel sont bloquées contre les accès des collaborateurs du responsable ou du sous-traitant qui, selon le principe de la minimisation des données conformément à l'article 5, alinéa 1, lettre c) du RGPD de l'UE, n'ont pas besoin d'avoir accès aux données pour le traitement licite des données. Pour ce faire, un concept d'habilitation par rotation ou basé sur un groupe est mis en place (cf. ci-dessus ainsi que A n° 3 et 8).

S3. Dispositions particulières en matière de procédure qui, dans le cas d'une transmission ou d'un traitement à d'autres fins, garantissent le respect des prescriptions de cette loi ainsi que la directive (UE) 2016/679

En cas d'exigences particulières en matière de protection des données par le biais de dispositions légales, sectorielles, conformes aux statuts ou contractuelles, les mesures de protection sont abordées avec le responsable dans un cas particulier et adaptées en fonction du niveau de protection nécessaire. Cela peut également comprendre le respect de certaines normes en matière de protection et de sécurité des données (ISO 27001, norme de protection de base BSI 200-1 à 200-3, loi sur le contrôle de sécurité, répartitions dans les catégories de protection des documents dans le service public etc.)

Les autres points de l'article 22, alinéa 2 BDSG sont déjà traités par les prescriptions de la directive (cf. ci-dessus A n° 1 à 8).

Annexe 2 du contrat de sous-traitance

Concrétisation des types de données, catégories de données et personnes concernées par le traitement

- Concrétisation des types et catégories de données :
  - Données de base client (par exemple informations de contacts des clients, adresses, etc.)
  - Données de référence (par exemple conditions de paiement et de livraison, coordonnées bancaires, etc.)
  - Données structurelles à l'échelle de l'entreprise (par exemple produits, services, responsabilités des employés, etc.)
  - Données de transaction (par exemple activité commerciale, etc.)

- Concrétisation des personnes concernées par le traitement :
- Clients et leurs employés (personne de contact)

Annexe 3 du contrat de sous-traitance

Sous-traitants autorisés :