QUESTIONNAIRE RELATIEF AUX MESURES TECHNIQUES ET ORGANISIONNELLES APPROPRIÉES
Annexe 2 du modèle de contrat de sous-traitance

Identification

Nom de l'organisation	Corilus NV / SA Rue Camille Hubert 23, 5032 Gembloux KBO 0428.555.896
Coordonnées de contact	Les coordonnées du point de contact pour la sécurité de l'information (CISO) et la protection des données (DPD) peuvent être consultées via le site https://www.corilusgdpr.com/fr/corilus/securitedesdonnees ou à tout moment en appelant le numéro de téléphone général de Corilus.
Version	v2.0 (23/04/2021)

Aperçu des mesures

Question	Uniquement d'application dans le cas où le hosting est fait chez Corilus	Mesure	Etat
1		Disposez-vous d'une politique de sécurité de l'information formelle et actualisée, approuvée par conseil d'administration ?	Oui, nous avons une politique de sécurité de l'information et de protection des données. Ces deux documents sont mis à jour et réaffirmés chaque année.
2		Disposez-vous d'un processus d'évaluation des risques pour chaque processus/projet touchant à la sécurité de l'information / protection des Données que vous utilisez pour la fourniture des prestations de services ?	Oui. Malgré le scope du certificat ISO-27001, les processus d'évaluation des risques sont en place pour toutes les équipes et toutes les unités busines. Cette évaluation couvre à la fois la protection des données et la sécurité de l'information.
3		Votre organisation a-t-elle, en son sein: Organisé un service chargé de la sécurité de l'information placé sous l'autorité fonctionnelle et directe du conseil d'administration ?	Oui, nous avons une équipe Qualité & Conformité de 2 personnes qui, en plus de la qualité et de la protection des données, sont également activement engagés dans la sécurité de l'information (par exemple: ISO-27001, le traitement des incidents et la monitoring des risques). Le Quality & Compliance Manager rend compte directement aux direction.
4		Disposez-vous d'un plan de sécurité de l'information approuvée par le conseil d'administration ?	Oui, nous disposons d'un registre des risques dans lequel tous les risques connus sont inclus après identification, analyse et évaluation. Le lien avec le traitement (et donc les mesures appropriées) est également inclus. Les mesures qui ne sont pas encore efficaces sont planifiées et suivies par le biais du registre des risques.
5		Combien d'heures sont prestées par le CISO et le DPD ? 1) CISO 2) DPD Combien d'heures de formation relative à la sécurité de l'information le CISO et le DPD ont-ils suivies ? 3) CISO 4) DPD	1) Au moins 120 heures / mois (sauf maladie, vacances ou autre absence) 2) Au moins 64 heures / mois (sauf maladie, vacances ou autre absence) 3) Au moins 40 heures / an 4) Au moins 40 heures / an Nous disposons également d'une équipe de qualité et conformité de 2 personnes. Ils gèrent entre autres la sécurité de l'information et la protection des données et soutiennent le CISO et le DPD dans leurs tâches.
6		Prenez-vous les mesures adéquates afin que les Données sensibles, confidentielles et professionnelles enregistrées sur des médias mobiles ne soient accessibles qu'aux seules personnes autorisées ?	Oui, les dispositifs mobiles tels que les clés USB, les CD, les DVD et les disques durs externes ne doivent être utilisés que dans les situations où les connexions réseau ne sont pas disponibles ou lorsqu'il n'existe pas d'autre méthode sûre de transfert de données. Lors du transfert de données sensibles ou confidentielles, la politique de transfert de données exige l'utilisation de dispositifs de stockage mobiles autorisés et dotés d'un cryptage (par exemple AES-256 bits).

7		Prenez-vous les mesures adéquates, en fonction du moyen d'accès, afin de garantir la sécurité de l'information de l'accès réalisé en dehors de votre organisation aux données sensibles, confidentielles et professionnelles ?	Oui, les employés qui font du télétravail sont soumis aux règles applicables de la politique d'utilisation acceptable, de la politique de classification des données et de la politique de transfert des données. L'accès aux sources de données n'est possible qu'en utilisant une connexion VPN ou en se connectant à l'aide d'une authentification multifactorielle. Le niveau de connexion et de cryptage de la connexion est lié à la classification de la source de données.
8		Avez-vous organisé les dispositifs de télétravail de l'organisation de sorte que sur le lieu du télétravail (à domicile, dans un bureau satellite ou à un autre endroit) aucune information ne soit enregistrée sur des appareils externes sans cryptage et qu'aucune menace potentielle ne puisse atteindre l'infrastructure IT au départ du lieu de télétravail ?	Oui. Les employés qui font du télétravail sont soumis aux règles applicables de la Politique d'utilisation acceptable, de la Politique de classification des données et de la Politique de transfert des données, qui font notamment référence au fait qu'aucune donnée ne peut être stockée localement et que les données doivent être traitées en fonction de leur classification (par exemple, jamais d'informations confidentielles sur un média non sécurisé).
9		Sensibilisez-vous tout collaborateur à la sécurité de l'information et la protection des Données et réalisez-vous annuellement une évaluation du respect de cette politique dans la pratique ?	Oui, il existe un programme de sensibilisation continue avec un plan par année civile qui tient compte à la fois des questions de protection des données et de sécurité de l'information. Chaque année, plusieurs activités sont menées pour sensibiliser les gens et leur rappeler leurs responsabilités.
10		Effectuez-vous une analyse annuelle concernant le respect de la politique de sécurité d'l'information et de protection des données dans la pratique ?	Oui. Des audits internes sont prévus chaque année pour la sécurité de l'information et pour la GDPR. Des audits externes ont lieu en ce qui concerne les certifications telles que le certificat ISO-27001. En outre, des investissements sont réalisés pour effectuer des tests de pénétration sur les infrastructures et les applications.
11		Avez-vous sécurisé l'accès par un dispositif d'accès précis et avez-vous implémenté un système d'accès (physique ou logique) afin d'éviter tout accès non autorisé en ce qui concerne les Données sensibles hébergées dans les centres de données ?	Oui. Une procédure d'accès au centre de données a été élaborée pour chaque centre de données. Nos centres de données certifiés ISO-27001 sont également mentionnés sur cette page.
12		Avez-vous sécurisé l'accès par un dispositif d'accès précis et avez-vous implémenté un système d'accès (physique ou logique) afin d'éviter tout accès non autorisé en ce qui concerne les Données sensibles hébergées dans les bâtiments administratifs ?	Oui. En termes d'accès logique, une politique de "gestion des accès" a été mise en place pour assurer, entre autres, l'utilisation d'une matrice d'accès, la séparation des droits et la gestion structurelle du cycle de vie du compte. En termes d'accès physique, chacun de nos bâtiments administratifs est équipé d'un système de badges, d'une alarme et d'un bureau d'accueil ouvert pendant les heures de bureau. Des caméras de sécurité ont également été installées. La politique d'utilisation acceptable rappelle également aux employés de ne pas stocker de données dans les médias locaux. En ce qui concerne notre service du personnel et la gestion des contrats, un espace séparé a été aménagé dans le bâtiment de Gand où les documents sont conservés dans une zone sécurisée. L'accès n'est possible qu'avec un badge d'accès et est limité aux personnes autorisées.
13	**X**	Disposez-vous d'un schéma de classification pour les données à caractère personnel pour lesquelles vous prestez des services et appliquez-vous ce schéma de classification ?	Oui, nous avons une politique de classification des données dans laquelle quatre niveaux sont élaborés (public, interne, confidentiel, sensible). Celles-ci sont appliquées (par exemple, les données sensibles ne peuvent être stockées que dans un centre de données certifié ISO-27001 et ne peuvent être transportées que par des canaux sécurisés.
14		Avez-vous intégré dans une politique relative à la sécurité de l'information les règles qui sont spécifiées dans une police 'E-mail, communication en ligne et utilisation d'internet' ?	Oui, nous avons une politique d'utilisation acceptable qui couvre entre autres le courrier électronique, la communication en ligne et l'utilisation d'Internet.
15		Avez-vous intégré dans une politique relative à la sécurité de l'information les règles qui sont spécifiées dans une police 'E-mail, communication en ligne et utilisation d'internet' ?	Oui, nous avons une politique d'utilisation acceptable qui couvre, entre autres, l'utilisation du courrier électronique, la communication en ligne et l'utilisation d'Internet. Il y est fait référence dans le règlement du travail. Ces mesures font également partie de l'intégration des nouveaux employés et de la sensibilisation périodique.
16		Lorsque vous souhaitez appliquer la 'cryptographie' : • Disposez-vous d'une politique formelle pour l'utilisation de contrôles cryptographiques ? • Disposez-vous d'une politique formelle pour l'utilisation, la protection et la durée de vie des clés cryptographiques pour le cycle de vie complet ?	Oui, nous avons une politique de cryptographie formelle et approuvée qui inclut ces deux points.
17		Prenez-vous des mesures de prévention nécessaires contre la perte, l'endommagement, le vol ou la compromission des actifs et contre l'interruption des activités ?	Oui, nous travaillons de manière proactive à la prévention et à la sensibilisation afin d'éviter les pertes, les dommages, les vols ou les compromis. Outre la prévention, nous travaillons également sur la détection (afin que nous en soyons informés) et le traitement approprié si de tels événements se produisent.
18		Déterminez-vous contractuellement avec le responsable du traitement les mesures appropriées pour la suppression ?	Oui. Selon l'article 28 de la GDPR, le client (responsable du traitement) et le fournisseur (sous-traitant) sont tenus de s'entendre sur un contrat de sous-traitance définissant les actions à la fin de l'accord (par exemple, l'exportation et/ou l'effacement). C'est le cas dans chacun de nos modèles de contrats de sous-traitance.

19		Appliquez-vous les règles relatives à la logging des accès telles que définies par le client ?	Si un client fournit des règles spécifiques concernant l'exploitation forestière, elles seront mises en œuvre et testées comme convenu au préalable. C'est particulièrement vrai lorsque nous livrons un projet.
20		L'ensemble des collaborateurs travaillent-ils avec des moyen ICT dans le cadre de la mission sur la base d'une autorisation minimale pour l'exécution de leurs tâches ?	Oui, nous avons une politique de gestion des accès qui stipule que les droits sont autorisés au minimum selon une matrice d'accès prédéfinie.
21		Les conditions de protection des accès (identification, authentification, autorisation) ont-elles été définies, documentées, validées et communiquées ? (1) Ces accès font-ils l'objet d'une prise de traces ? (2)	1) Oui 2) Voir la question 25
22		Le principe "data protection by design" est-il appliqué de telle sorte qu'au cours de la phase de développement du projet/développement de software les garanties nécessaires en faveur de la protection des Données à caractère personnel sont transposées ?	Oui. Afin d'accroître encore notre maturité, nous avons commencé à déployer une stratégie de sécurité des applications au 2021.
23		Les dispositifs de développement, de test et/ou d'acceptation, et de production sont-ils scindés sous la supervision du chef de projet/manager responsable concerné et le partage des responsabilités dans le cadre du projet/software qui en découle est-il réalisé ?	Oui. Dans tous nos projets, les environnements de développement, de test et/ou d'acceptation et de production sont clairement séparés les uns des autres.
24		Tout accès à des Données à caractère personnel et confidentielles fait-il l'objet d'une prise de logs, conformément à la politique de l'entreprise relative au "logging" et à la législation et à la réglementation Applicables ?	Oui, l'accès aux informations personnelles et confidentielles est régi par un système formel d'enregistrement des audits des politiques.
25		La journalisation (le « logging ») satisfait-elle au moins aux objectifs suivants ? • Les informations permettant de déterminer qui a obtenu accès à quelles informations, à quel moment et de quelle manière • L'identification de la nature des informations consultées • L'identification précise de la personne	Nos récentes applications (cloud) répondent aux exigences requis. Les anciennes applications (legacy) qui ne sont pas développées plus, ont mis en œuvre la logging au mieux de leurs possibilités.
26		Les outils nécessaires sont-ils disponibles pour permettre que les données de logs puissent être exploitées par les personnes autorisées (user interface of procédure) ?	Si le point précédent "oui", ici aussi "oui". Nous entendons par là que si des journaux sont disponibles, ils peuvent être consultés dans les applications via l'interface utilisateur, des fichiers texte ou une base de données.
27		Les données de logs transactionnelles/fonctionnelles sont-elles conservées conformément aux données à caractère personnel elles-mêmes (p. ex. 30 ans pour les données médicales) ?	Si le question précédent est "oui", ici aussi "oui".
28		Les délivrables du projet (les Données qui sont traitées, la documentation (code source, programmes, documents techniques, ...) du projet/processus de développement du software sontils intégrés dans le système de gestion des sauvegardes ?	Oui. Tous les artefacts pertinents de l'ensemble du cycle de développement sont soumis à des exigences de sauvegarde.
29		Au cours du développement du projet/du software, les besoins relatifs à la continuité de la prestation de services sont-ils formalisés conformément à vos attentes ?	Pour nos projets de consultation, nous tenons toujours compte des exigences fonctionnelles et non fonctionnelles nécessaires en matière de continuité (par exemple, robustesse, redondance, sauvegarde, correctifs, procédures, ...).
30	**X**	Votre plan de continuité et les procédures y afférentes, en ce compris les tests de continuité, sontils actualisés en fonction de l'évolution du projet/software ?	Notre équipe Cloud Operations ("DevOps") dispose d'un plan de continuité formel (y compris le DRP avec les procédures associées, les tests DRP, le wiki actif, la surveillance) qui relève de la norme ISO-27001 et qui a été évalué par l'auditeur externe. Ces questions sont également présentes chez nos fournisseurs de centres de données. Pour les applications qui ne sont pas proposées par l'équipe Cloud Operations, des procédures de continuité sont disponibles, qui évoluent avec le logiciel et les exigences des clients.
31	**X**	Une analyse des risques est-elle réalisée au début du projet (de développement de software) afin de définir les procédures d'urgence, compte tenu de la "data protection by design" ?	Oui. Malgré le scope du certificat ISO-27001, les processus d'évaluation des risques sont en place pour toutes les équipes et toutes les unités commerciales. Cette évaluation couvre à la fois la protection des données et la sécurité de l'information. Des lignes directrices ont été élaborées autour des principes de "protection des données par conception et par défaut".
32		Les procédures relatives à la gestion des incidents sont-elles formalisées et validées ?	Oui, nous disposons d'une procédure formelle de gestion des incidents qui couvre à la fois le traitement d'un incident de sécurité et d'une violation de données.
33	**X**	Le CISO est-il informé des incidents relatifs à la sécurité et le DPO est-il informé des incidents relatifs à la protection des Données ?	Oui, chaque incident de sécurité présumé est communiqué au CISO, au DPD et aux membres de l'équipe Qualité et conformité. Il y aura également une communication transparente à ce sujet avec l'équipe de direction et, éventuellement, avec notre conseil d'administration.
34		La documentation (technique, procédures, manuels, ...) est-elle actualisée au cours de la durée de vie du projet / du software ?	Oui, chaque équipe de développement a une obligation de documentation et doit donc créer et maintenir des procédures techniques, des diagrammes et des manuels pertinents, entre autres. Nombre de nos applications les publient également sur Internet à l'intention des clients et des intégrateurs.
35		Tous les actifs, en ce compris les systèmes acquis ou développés, sont-ils ajoutés à l'inventaire des moyens opérationnels (asset mgt) ?	Oui. Tous les actifs d'exploitation sont enregistrés dans un inventaire. Cela comprend tous les ordinateurs portables, serveurs, composants d'infrastructure et applications ICT.

36		La collaboration appropriée est-elle apportée aux audits effectués sous la forme de mise à la disposition du personnel, de la documentation, de la gestion des traces et des autres informations qui sont raisonnablement disponibles ?	Oui. Selon l'article 28 de la GDPR, le client (responsable du traitement) et le fournisseur (sous-traitant) sont tenus de s'entendre sur un contrat de sous-traitance définissant les possibilité d'audit et notre coopération. C'est le cas dans chacun de nos modèles de contrats de sous-traitance.
37		Les conditions relatives à la sécurité de l'information et à la protection des Données sont-elles documentées afin de réduire les risques relatifs à l'accès aux moyens d'informations ?	Oui. Dans le cadre de notre ISMS et des politiques, procédures et manuels associés, les exigences sont résumées pour les applications en vue d'une mise en œuvre sécurité par conception et vie privée par conception (et par défaut). Chaque application développée comporte des cas d'utilisation définis autour de ces deux thèmes.
38		Toutes les conditions pertinentes relatives à la sécurité de l'information et à la protection de la vie privée font-elles l'objet d'un accord entre vous et les tiers (qui lisent, traitent, enregistrent, communiquent des informations de l'organisation ou qui fournissent des éléments d'infrastructure ICT et des services ICT) ?	Oui, chaque fournisseur agissant en tant que sous-traitant secondaire (c'est-à-dire traitant les données personnelles de nos clients et de leurs patients/résidents) conclut un accord avec le sous-traitant, dans lequel les exigences pertinentes en matière de sécurité de l'information (par exemple, prendre des mesures appropriées, cf. art. 32 du RGPD) et de protection des données (cf. art. 28 du RGPD) sont convenues.
39		Les prestations de service de tiers/ Sous-traitants font-elles l'objet d'un monitoring et sont-elles évaluées et auditées à intervalles réguliers ?	Un processus global de gestion du cycle de vie des contrats a été mis en place. Tous les fournisseurs sont également contrôlés, évalués et audités régulièrement sur la base d'un questionnaire. Pour les applications qui relèvent du certificat ISO-27001, une politique de sécurité des fournisseurs a également été activé.
40	**X**	Lorsque vous souhaitez traiter des Données sensibles, confidentielles ou professionnelles dans un cloud, satisfaites-vous aux garanties contractuelles minimales ?	Oui, tant notre cloud privé que les fournisseurs de cloud respectent des garanties contractuelles concernant le cloud.
41		Disposez-vous de procédures pour la détermination et la gestion d'incidents relatifs à la sécurité de l'information ou à la protection des Données et des responsabilités y afférentes et avez-vous communiqué ces procédures en interne ?	Oui, nous avons une procédure d'incident claire qui tient compte à la fois des violations de la sécurité ("'incident de sécurité") et des violations des données personnelles ("fuite de données").
42		Avez-vous signé un contrat avec tous les collaborateurs dans lequel il est stipulé que tout collaborateur (fixe ou temporaire, interne ou externe) est obligé de signaler tout accès, utilisation, modification, publication, perte ou destruction non autorisés d'informations et de systèmes d'information ?	Oui, la réglementation du travail a été mise à jour avant l'entrée en vigueur du GDPR pour inclure l'obligation de signalement interne des événements négatifs (suspectés) tels qu'un incident de sécurité ou une violation de données.
43		Les événements et faiblesses relatifs à la sécurité de l'information ou à la protection des Données en rapport avec les informations et les systèmes d'information sont-ils rendus publics, de sorte que vous puissiez prendre, en temps utile, des mesures correctrices adéquates ?	Oui. Conformément aux dispositions de la convention de traitement et de l'article 28 du RGPD en général, nous, en tant que sous-traitants, sommes tenus d'informer nos clients (en leur qualité de responsables du traitement) sans délai déraisonnable de tout événement négatif relatif à des données à caractère personnel si celui-ci peut entraîner un risque. Ceci est inclus dans notre politique et les procédures associées.
44		Les incidents relatifs à la sécurité de l'information ou à la vie privée sont-ils rapportés, dans les meilleurs délais, par l'intervention du supérieur hiérarchique, l'helpdesk, ou du conseiller en sécurité de l'information (CISO) ou du Délégué à la protection des Données (DPD) ?	Oui. Conformément aux dispositions de la convention de traitement et de l'article 28 du RGPD en général, nous, en tant que sous-traitants, sommes tenus d'informer nos clients (en leur qualité de responsables du traitement) sans délai déraisonnable de tout événement négatif relatif à des données à caractère personnel si celui-ci peut entraîner un risque. Ceci est inclus dans notre politique et les procédures associées.
45		Est-ce que les preuves, relatives aux incidents concernant à la sécurité de l'information ou à la vie privée, sont collectées conformément aux lois et règlements en vigueur ?	Oui. Les registres pertinents et tout élément pouvant être considéré comme une preuve sont collectés et traités de manière appropriée, conformément aux exigences applicables.
46		Tout incident relatif à la sécurité de l'information ou à la protection des Données est-il validé de manière formelle, de sorte que les procédures et mesures de contrôle puissent être améliorées ? Les leçons tirées d'un incident sont-elles communiquées à votre direction, en vue de la validation et de l'approbation d'actions futures ?	Oui, chaque incident de sécurité et chaque violation de données est lié à des actions d'amélioration. Nous disposons également d'un certificat ISO-27001 valide, qui souligne l'aspect de l'amélioration continue. Nous intégrons ces fonctionnements dans notre ADN.
47		Dressez-vous régulièrement la carte des risques relatifs à la conformité au RGPD et exécutez-vous les actions devenues nécessaires suite à un risque "résiduel" majeur de non-conformité ?	Oui, au moins un audit de GDPR a lieu chaque année et tous les points qui ressortent de ce rapport sont repris et communiqués à l'équipe de direction.
48		Disposez-vous d'un registre central mis à jour du responsable du Traitement ou du sous-traitant et possédez-vous une justification formelle de la non-réalisation des mesures de contrôle axées sur le respect du RGPD pour le Traitement spécifique ?	Oui, nous traitons des données à caractère personnel en tant que responsable du traitement (par exemple, rôle d'employeur) et en tant que sous-traitant pour nos clients (par exemple, hébergement, back-up service, support). Un registre de traitement distinct a été créé pour les deux rôles, qui est conforme à la RGPD-Art. 30.