

QUESTIONNAIRE RELATIF AUX MESURES TECHNIQUES ET ORGANISATIONNELLES APPROPRIÉES

Annexe 2 du modèle de contrat de sous-traitance

Identification

Nom de l'organisation	Corilus NV / SA Gaston Crommenlaan 4 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.corilugdpr.com/corilus/databeveiliging ou à tout moment en appelant le numéro de téléphone général de Corilus.
Version	v3.0 (26/06/2024)

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 lors d'un examen formel de la direction.
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. Tous les processus relatifs à l'évaluation des risques sont en place et s'appliquent à toutes les équipes de l'organisation, comme le prévoit notre ISMS. 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 disposons d'une équipe chargée de la qualité et de la conformité, qui comprend un CISO et un DPO. Cette équipe rend compte directement à l'équipe de 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		L'organisation a-t-elle nommé un CISO et un DPO ? Le CISO et le DPO bénéficient-ils de possibilités de formation suffisantes en matière de sécurité de l'information et de protection des données ?	Nous disposons d'un CISO et d'un DPD à temps plein au sein de l'organisation (voir question 3). Comme il s'agit de postes cruciaux au sein de l'organisation, un budget et un temps suffisants ont été prévus pour leur permettre de suivre les cours de formation nécessaires.
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
9		Sensibilisez-vous chaque année vos employés à la sécurité de l'information et à la protection des données ?	Oui, il existe un programme de sensibilisation continue 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'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 politique 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 ?	En ce qui concerne l'accès logique, une politique de 'gestion des accès' a été introduite pour garantir, entre autres, l'utilisation d'une matrice d'accès, la séparation des droits et la gestion structurelle du cycle de vie des comptes.
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). Ces niveaux sont appliqués (par exemple, les données sensibles ne doivent être stockées que dans un centre de données certifié ISO-27001 et ne doivent 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 traitement du courrier électronique, la communication en ligne et l'utilisation de l'internet. En outre, cette politique est également incluse dans le règlement sur l'emploi. Elles font également partie de l'intégration des nouveaux employés et de la sensibilisation périodique.
15		Les employés ont-ils un obligation de discrétion et de confidentialité ?	Oui, cela est mis en œuvre à la fois par la réglementation du travail et par le contrat de travail.
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 disposons d'une politique officielle et approuvée en matière de cryptographie qui couvre 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).
19		La journalisation du contrôle d'accès est-elle suffisante dans les applications utilisées par le responsable du traitement ?	Dans le cadre de notre ISMS, nous disposons d'une politique de journalisation et de surveillance qui définit les règles minimales à respecter en ce qui concerne la génération et le stockage des journaux. Cette politique est alignée sur la réglementation applicable.

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 en matière de sécurité de l'accès (identification, authentification, autorisation) sont-elles définies, documentées, validées et communiquées ?	Oui, nous disposons des documents de politique générale nécessaires à cet effet dans le cadre de notre système de gestion de l'information (ISMS). Ceux-ci contiennent les exigences de sécurité nécessaires en matière de sécurité d'accès.
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. Les exigences en matière de sécurité et de protection des données sont mises en œuvre par le biais de divers documents de politique au sein de notre ISMS. Afin d'accroître notre maturité, nous mettons continuellement à jour notre stratégie de sécurité des applications et révisons régulièrement nos exigences.
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 ?	En outre, certaines de nos applications (voir ehealth) sont conformes aux critères d'homologation imposés, y compris les règles relatives à la sécurité de l'accès.
24		Tous les événements (CRUD) au sein de l'application sont-ils enregistrés conformément aux lois et réglementations 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 ? <ul style="list-style-type: none"> • 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 	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 livrables du projet (les données qui sont traitées, la documentation, code source; documents techniques, ...) du projet/processus de développement du software sont-ils 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.
28		Au cours du développement du projet/du software, les besoins relatifs à la continuité de la prestation de services sont-ils formalisés?	Nous prenons toujours en considération les exigences fonctionnelles et non fonctionnelles nécessaires en matière de continuité (par exemple, robustesse, redondance, sauvegarde, correctifs, procédures, etc.)
29	x	Votre plan de continuité et les procédures y afférentes, en ce compris les tests de continuité, sont-ils 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 a été évalué en tant que tel par l'auditeur externe. Ces éléments sont également en place chez nos fournisseurs de centres de données.
30	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".
31		Les procédures relatives à la gestion des incidents sont-elles formalisées, validées et communiquées en interne ? Ces procédures permettent-elles de communiquer/rapporter en interne les incidents liés à la sécurité de l'information/protection des données dans les meilleurs délais ?	Oui, nous disposons d'une procédure formelle de gestion des incidents qui traite à la fois de la gestion d'un incident de sécurité et d'une violation de données à caractère personnel. Des sessions de sensibilisation appropriées sont organisées au sein de l'organisation à cette fin.
32	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. Toute suspicion de violation de la sécurité ("incident de sécurité"), telle qu'une violation de données à caractère personnel ("fuite de données"), est communiquée au CISO, au DPO 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.

33		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.
34		Tous les actifs, en ce compris les systèmes acquis ou développés, sont-ils ajoutés à l'inventaire des moyens opérationnels (asset management) ?	Oui. Tous les actifs d'exploitation sont enregistrés dans un inventaire. Cela comprend tous les ordinateurs portables, serveurs, composants d'infrastructure et applications ICT.
35		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 possibilités d'audit et notre coopération. Ceci est également documenté comme tel dans notre accord standard avec le processeur.
36		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.
37		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.
38		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. Une politique de sécurité des fournisseurs s'applique également au ISMS.
39	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.
40		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.
41		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.
42		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.
43		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 en fonction du risque ?	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.
44		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.
45		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.