Attestation : disposition pour la protection des données - RGPD

Règles de confidentialité et contrôle de leur application

Les meilleures pratiques d'évaluation, d'audit et de certification de produits, de processus, de services et de systèmes de management de la qualité sont entre autres définies respectivement dans la norme internationale ISO 17065:2012 « Evaluation de la Conformité – Exigences pour les organismes certifiant les produits, les procédés et les services » et dans la norme internationale ISO 17021-1:2015 « Evaluation de la conformité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management – Partie 1 : Exigences ». L'article 4.5 de la première norme et les articles 8.4.7 et 9.9.3 de la seconde norme décrivent les exigences relatives au traitement sécurisé des informations confidentielles.

CertUp est accrédité pour le Référentiel National Qualité « Qualipoi » selon la première norme par le COFRAC, sous le numéro 5-0614. Le COFRAC est l'organisme français d'accréditation signataire des accords de reconnaissances mutuelles internationales. CertUp est périodiquement contrôlé suivant cette norme et en particulier sur les exigences relatives à la confidentialité des données. La validité de son accréditation peut être vérifiée à tout moment sur www.cofrac.fr. CertUp en Belgique bénéficie de l'accréditation suivant la seconde norme - et ce y compris couvrant les exigences relatives à la confidentialité des données - portant le numéro 600-QMS de l'organisme belge d'accréditation BELAC du Ministère des Affaires Economiques, signataire des accords de reconnaissances mutuelles internationales. La portée de sa validité peut être vérifiée à tout moment sur le site de BELAC.

Les procédures relatives à la confidentialité des données sont identiques pour CertUp en France et en Belgique et couvrent l'ensemble des activités de certification et des activités d'analyse et d'évaluation de la conformité. Ces dernières pouvant être réalisées au profit de et sous la responsabilité de CertUp par un sous-traitant qui est soumis aux mêmes règles faisant l'objet de contrôle. Ceci vaut en particulier pour Maïeutika.

Transfert et traitement des données confidentielles

Le règlement d'audit qui fait partie intégrante de la convention d'audit précise quelles sont les données à caractère public et quelles sont les données à caractère confidentiel.

Pour le transfert sécurisé de fichiers informatiques confidentiels, l'organisme audité est invité à faire usage de la fonctionnalité prévue à cette fin dans l'application en ligne auquel il reçoit l'accès.

Les procédures internes de CertUp prescrivent la manière selon laquelle les données confidentielles nécessaires à la réalisation des audits sont gérées. Ceci se fait au sein de l'Union européenne, exclusivement par les personnes qui par leur fonction ou leur responsabilité ont un rôle à jouer dans la réalisation des audits, et uniquement à cette fin. Chacune de ces personnes est liée par un contrat reprenant une clause spécifique garantissant la confidentialité des données d'audit et des données confidentielles reçues d'organismes audités. Le règlement d'audit, les procédures internes et les contrats des personnes ont été soumis aux contrôles du COFRAC. Ces documents eux-mêmes sont adaptés des documents de la maison-mère CertUp SA, accrédité par BELAC.

A la clôture de la mission de certification, les données confidentielles tant papier qu'électroniques non nécessaires à la traçabilité de l'exécution de l'audit sont détruites. Les données archivées à des fins de traçabilité de la réalisation de la mission d'audit sont conservées sur des serveurs sécurisés et les données papier sont conservées dans un système d'archivage à accès sécurisé. Conformément au § 9.9.4 de la norme ISO 17021-1 :2015, les données confidentielles nécessaires sont conservées durant tout le cycle de certification plus la durée d'un cycle supplémentaire ; soit au total six années.

Procédure en cas de violation de données

CertUp dispose d'une Politique interne de la Sécurité de l'Information « Information Security Policy » applicable contractuellement à tous ses collaborateurs et sous-traitants et à laquelle ils ont été spécifiquement formés. Celle-ci est établie suivant la structure de l'ISO 27001 :2013 « Information technology – Security techniques – Information security management systems – Requirements ». Si malgré toutes les mesures prises une violation de données devait avoir lieu, CertUp s'engage à avertir l'organisme audité dans les 24 heures de son constat en communiquant toutes les informations utiles sur les circonstances de la violation, ses conséquences et les mesures prises pour y remédier. Par ailleurs, CertUp et ses éventuels sous-traitants communiquent clairement dans leurs documents et sur leur site web que toute question relative à la vie privée peut leur être adressée à privacy@maninfo.be.

Application par CertUp des documents et exigences de l'organisme client

Les engagements repris dans la convention d'audit et le règlement d'audit sont établis dans le respect des législations en vigueur. Les prix d'audit repris dans les offres sont des prix nets correspondant à ces engagements. Si l'organisme souhaite utiliser ses propres documents et exigences en remplacement ou en complément, une nouvelle offre de prix sera établie pour l'étude et/ou la mise en conformité avec ces exigences.

Pour CertUp SARL, le 27/10/2021, Dominique Delferrière, Gérant

CertUp POWERED by Qfor