Sécurité de l'Information

KPMG

Mars 2019

Sommaire

Introduction

Ce document a pour objectif de présenter les pratiques adoptées par KPMG SA, société anonyme de droit français, dont le siège social se situe Tour Eqho, 2 avenue Gambetta CS 60055 – 92066 Paris La Défense Cedex, les entités qu'elle détient et contrôle en France, ainsi que KPMG Avocats, KPMG Academy, KPMG Associés et la Fondation d'entreprise KPMG France (ci-après, "KPMG" ou, collectivement, le "cabinet") en matière de sécurité de l'information et de protection des données.

KPMG s'engage à maintenir un environnement sûr et fiable pour les données personnelles et les informations confidentielles qui lui sont confiées, et à protéger toutes données à caractère privé de ses clients, fournisseurs et tiers.

KPMG considère que ces informations et les systèmes d'informations qui y sont associés sont des atouts précieux et essentiels à son activité. Grâce à des ressources dédiées visant à améliorer les pratiques en matière de sécurité de l'information, KPMG s'engage à identifier les risques inhérents à ses données et se protéger de tout accès non autorisé, de toute perte, ou toute utilisation non conforme. Dans le cadre de la gestion de ces risques, KPMG a mis en place différents dispositifs de contrôle d'accès, de sécurité, et des outils d'évaluation pour analyser ses systèmes et réseaux.

Les politiques et pratiques du cabinet sont communiquées à tout le personnel. Des brochures d'information, des campagnes de sensibilisation et des formations renforcent l'adoption de ces pratiques. KPMG a mis à disposition la politique de sécurité de l'information à tout son personnel. Cette politique exige que les collaborateurs utilisent les ressources informatiques de KPMG de façon appropriée, et met l'accent sur le respect de la protection des informations personnelles et confidentielles de tout employé, de KPMG, et des clients. Le respect des politiques et procédures relatives à la sécurité de l'information est évalué régulièrement.

Tous les collaborateurs de KPMG respectent la loi et adhèrent aux normes professionnelles applicables et aux exigences en matière d'éthique, imposées par les instances représentatives des professions concernées par l'activité de KPMG (Ordre des Experts-Comptables, Compagnie Nationale des Commissaires aux Comptes, Conseil national des barreaux), par les organismes qui les règlementent (Haut Conseil du Commissariat aux Comptes, Autorité des Normes Comptables, Chancellerie, Conseil national des barreaux) et par les organismes de règlementation du système financier et fiscal. Certains règlements sont applicables au cabinet et à ses collaborateurs, et prennent en compte les spécificités propres à chaque client (notamment l'Autorité des marchés financiers et l'Autorité de contrôle prudentiel). De plus, tous les collaborateurs de KPMG ont une obligation contractuelle de respect des politiques de sécurité de l'information de KPMG.

Fonctions dédiées à la sécurité de l'information

L'équipe responsable de la sécurité de l'information de KPMG est composée notamment de professionnels travaillant dans les départements du Risk Management et Informatique (« ITS »). Elle est chargée de faire évoluer et soutenir les pratiques en matière de sécurité de l'information de KPMG, par le biais d'activités de sensibilisation et de formation, de participer à l'évolution des normes applicables, et de l'évaluation de la sécurité informatique et des risques. En travaillant en étroite collaboration avec les différents métiers de KPMG, les professionnels de l'information élaborent des normes appropriées visant à assurer la sécurité de ses informations ainsi que celles de ses clients. Grâce à ces différentes activités, le personnel de KPMG dispose d'outils et de ressources lui permettant de comprendre sa responsabilité vis-à-vis de la sécurité et de la protection des informations de ses clients.

Sécurité de l'information : activités clés

- Mettre en place des politiques et accompagner les utilisateurs dans le cadre de l'exploitation des données, du matériel, du réseau et des systèmes informatiques de KPMG.
- Développer des stratégies et des normes, et mettre au point des contrôles de sécurité afin de protéger les informations propres à nos clients et toute autre information présente dans les systèmes de KPMG.
- Apporter des conseils sur la gestion des risques.
- Gérer les dispositifs de contrôle de la sécurité informatique et veiller à ce qu'ils respectent les normes et les politiques de KPMG International.
- Gérer le programme de conformité, notamment :
- Effectuer des bilans sur la sécurité de l'information et évaluer les risques. Faciliter le contrôle interne du département ITS et des bureaux de KPMG.
- Comprendre l'impact des nouvelles lois et réglementations sur l'environnement informatique.
- Entreprendre un programme d'activités de sensibilisation et de formation pour veiller à ce que les collaborateurs comprennent leurs responsabilités vis-à-vis de la protection des clients, des données personnelles et de KPMG.

Politiques et normes

Sécurité de l'information

Le dispositif de sécurité de l'information de KPMG repose sur un éventail complet de politiques, normes et processus. Ces derniers comprennent notamment :

- Organisation de la sécurité
- Politique sur la sécurité
- Responsabilité vis-à-vis des biens
- Sécurité du personnel
- Gestion de la continuité des opérations
- Sécurité physique et de l'environnement
- Gestion des incidents de sécurité de l'information
- Contrôle des accès
- Développement des systèmes
- Conformité

Confidentialité client

Le personnel de KPMG est soumis aux politiques de confidentialité, conformément au code de conduite et au manuel « Quality and Risk Management », et aux politiques internes relatives à l'utilisation et la diffusion des informations propres aux clients. Ces politiques englobent les règles et principes de confidentialité prévus par la loi et les organismes de règlementation des professions de i) commissaire aux comptes, dont l'article L.822-15 du code de commerce, l'article 9 du code de déontologie de la profession de commissaire aux comptes et l'article 622-1 du règlement général de l'autorité des marchés financiers, ii) expert-comptable, dont la section 140 du code de déontologie des professionnels comptables, l'article 21 de l'ordonnance n° 45-2138 du 19 septembre 1945 et l'article 147 du décret n°2012-432 du 30 mars 2012 et iii) avocat, dont l'article 66-5 de la loi n° 71-1130 du 31 décembre 1971 et les dispositions du RIN (Règlement Intérieur National de la profession d'avocat).

Dans le cas où KPMG autorise un tiers à exploiter les informations confidentielles ou à caractère personnel en son nom, le contrat conclu avec ce tiers stipule que ce dernier a un devoir de confidentialité dans l'utilisation de toutes les informations privées et confidentielles, conformément aux politiques et pratiques de KPMG relatives à la confidentialité en particulier.

Contrôles

Contrôles d'accès

KPMG a mis en place des mesures de sécurité visant à gérer et contrôler l'accès physique aux locaux qui hébergent l'information de KPMG et de ses clients. L'accès à ses bureaux est limité aux personnes autorisées utilisant des dispositifs électroniques ou mécaniques de contrôle d'accès, ou aux visiteurs autorisés. De plus, l'accès aux centres de données est limité aux seules personnes autorisées ou aux visiteurs, devant signer un journal d'entrées, et être accompagnés en permanence.

Conformément aux exigences de sécurité de l'information de KPMG, les règles relatives à l'accès aux applications professionnelles sont définies par les propriétaires des applications professionnelles et adoptent le principe de séparation des privilèges. La politique de sécurité informatique de KPMG prévoit l'ajout, la modification et la suppression de comptes utilisateurs lorsque des collaborateurs intègrent KPMG, lorsqu'ils changent de poste ou lorsqu'ils quittent le cabinet. Le personnel de KPMG qui travaille hors des bureaux de KPMG a accès à son réseau et ses ressources via le réseau privé virtuel (VPN) seulement, après une double authentification. KPMG sensibilise régulièrement son personnel sur les responsabilités qui lui incombent vis-à-vis de la sécurité de l'information.

Contrôles techniques

Le dispositif de sécurité de l'information de KPMG permet plusieurs niveaux de contrôle. Les applications utilisées hors du réseau local sont situées dans une partie séparée et sécurisée de l'infrastructure informatique, connue sous le nom de DMZ (zone démilitarisée). L'accès à la DMZ est restreint, ce qui limite l'utilisation non autorisée des applications hébergées dans cette partie du réseau.

KPMG a adopté un système de double pare-feu, qui permet d'isoler les applications internet utilisées hors du réseau local. Les points de connexion au réseau KPMG (tels qu'internet ou connexions dédiées) réservés aux tiers, sont protégés par un pare-feu. Tout changement de configuration du pare-feu est évalué en fonction des risques encourus, en conformité avec un processus spécifique. Les pare-feux sont des éléments essentiels du contrôle de la sécurité. Le dispositif de sécurité de KPMG comprend également plusieurs systèmes de contrôle complémentaires permettant de sécuriser le réseau de KPMG.

Lors de la configuration des ordinateurs personnels (PC), appareils portables, serveurs, matériel informatique et systèmes d'exploitation, le niveau de sécurité est assuré de façon homogène. Ces mesures de sécurité comprennent notamment : antivirus, chiffrement intégral des disques, chiffrement des supports externes, mises à jour et correctifs de sécurité, pare-feux, contrôles d'accès, suivi des événements, sécurité du réseau, expiration des autorisations d'accès, gestion des mots de passe et messages d'avertissement. Le cabinet évalue et améliore ces mesures de sécurité de façon régulière afin d'appliquer les pratiques en vigueur en matière de technologie et les normes régissant son secteur d'activité.

En fonction des exigences et des capacités informatiques de nos clients, des contrôles techniques supplémentaires peuvent être réalisés sur demande, tels que le chiffrement transparent des messages électroniques, la mise en place d'un site de collaboration sécurisé, et le transfert de données sécurisé (notamment le chiffrement des disques externes).

Contrôles dédiés aux projets

Dans le cadre du processus d'évaluation, nous analysons les nouveaux systèmes informatiques et leurs mises à jour afin de respecter le niveau de sécurité requis par KPMG, et de protéger les données confidentielles de ses clients de façon appropriée. Ce processus a pour objectif d'évaluer la fonctionnalité du système et identifier les risques pour la sécurité des informations au sein du système. Si des risques sont identifiés, des mesures correctives sont élaborées et mises en place, lesquelles permettent de sécuriser toute donnée confidentielle appartenant aux clients avant qu'elle ne soit accessible ou utilisée.

Evénements de sécurité

Surveillance des évènements de sécurité informatique

Afin d'apporter une réponse appropriée aux événements de sécurité, KPMG dispose de plusieurs outils permettant d'évaluer les opérations effectuées sur ses systèmes et par son personnel. De plus, KPMG a mis en place un logiciel antivirus agissant sur plusieurs éléments du système (dont la messagerie électronique, les serveurs et les PC), ce qui permet la mise à jour automatique des définitions d'antivirus de manière régulière et la mise en place de plans de déploiement d'urgence, le cas échéant. Des processus automatisés permettent de bloquer les fichiers d'origine inconnue et identifier les intrusions possibles, protégeant l'environnement de KPMG de toute infection virale.

KPMG a mis en place des processus permettant de suivre les alertes de sécurité, afin d'identifier la vulnérabilité des systèmes et les programmes malveillants, tels que vers et virus informatiques. Ces processus impliquent l'analyse des risques pour l'environnement de KPMG, la mise à jour et l'installation de correctifs de sécurité, et la mise en place de mesures de protection, le cas échéant.

Les logiciels susceptibles de porter atteinte à l'intégrité des systèmes et réseaux de KPMG sont identifiés. Ces logiciels ne doivent pas être téléchargés sur les ordinateurs de KPMG ou utilisés sur le réseau. La liste des logiciels interdits inclut les systèmes « peer-to-peer » et de partage de fichiers, les messageries instantanées externes, et les utilitaires systèmes. Des procédures permettent d'effectuer des scans et des recherches, et d'établir des rapports sur les applications ou les logiciels installés sur des machines KPMG pouvant présenter un risque. Les rapports permettent d'identifier les utilisateurs concernés et de leur adresser une notification de suppression immédiate des logiciels ou applications non autorisés. Des sanctions disciplinaires pourront être appliquées à toute personne refusant de supprimer les logiciels ou applications interdits.

Incidents de sécurité

Des procédures permettent de gérer les incidents de sécurité, dont la perte / diffusion de données et les incidents de sécurité physique :

- Tout incident de sécurité informatique est communiqué au Responsable de la sécurité informatique.
- Tout incident impliquant des données est communiqué au département Risk Management et au Service juridique interne.
- Tout incident de sécurité physique est communiqué au Responsable de la sécurité physique.

Cycle de vie des données

Sauvegarde des données

Des processus de sauvegarde de données ont été mis en place afin de pouvoir récupérer les données suite à une panne système, ou de toute anomalie. Les données sont sauvegardées conformément aux règles de continuité des opérations et de reprise d'activité après une catastrophe. L'intégrité des données sauvegardées est testée régulièrement, conformément aux procédures de récupération des données.

Conservation et suppression

KPMG applique les politiques relatives à la conservation de documents, conformément à la loi, aux exigences réglementaires et aux exigences liées aux professions concernées par les activités de KPMG. Ces politiques sont applicables à tout type de document ou fichier, physique ou électronique. Après expiration de la période de conservation (de 7 à 10 ans selon la profession concernée), les documents ou fichiers sont supprimés de manière sécurisée, conformément aux normes régissant notre secteur d'activité et à nos politiques.

Mise au rebut du matériel

Les données contenues sur les PC et disques durs de KPMG arrivant en fin de vie sont effacés grâce au logiciel d'effacement des données « Blancco ».

Tous les serveurs arrivant en fin de vie sont recyclés de manière sécurisée par des professionnels agréés.

Conformité interne

L'équipe responsable de la sécurité de l'information de KPMG a mis en place un programme d'évaluation des risques internes, dédié notamment à la sécurité de l'information, comprenant :

- Une évaluation annuelle : constituée d'une auto-évaluation et d'un audit. L'auto-évaluation est basée sur le programme d'évaluation reconnu au niveau international (http://sharedassessments.org/). Elle permet d'assurer l'évaluation continue de la conformité de tous les cabinets membres de KPMG, vis-à-vis de la gestion de la sécurité de l'information et de la sécurité informatique. Elle est effectuée tous les ans par le Responsable de la sécurité informatique de chaque cabinet membre. Les résultats sont transmis à la Direction de chaque cabinet membre qui est responsable de la gestion de ces résultats. Le Département IPG (Protection de l'Information) de KPMG International est responsable du suivi.

- Une évaluation annuelle de la vulnérabilité informatique : le Département IPG de KPMG International met à disposition des cabinets membres des outils de détection de vulnérabilités sur toute infrastructure et logiciel exposés sur internet. Cette évaluation a pour objectif de mesurer le risque et d'identifier les correctifs et mesures de sécurité à mettre en œuvre.

Conformité avec les normes informatiques

Conformément aux politiques internes, KPMG respecte les normes informatiques et assure la maintenance des logiciels installés sur tous ses ordinateurs. Les normes informatiques, les versions des logiciels et les correctifs de sécurité sont régulièrement suivis et évalués par le Département informatique qui s'assure de leur validité et de leur mise à jour ou les remplace si nécessaire. Les produits et logiciels inclus dans la configuration standard des ordinateurs de KPMG sont mis à jour et déployés sur toutes les plateformes, dans le cadre du déploiement effectué au niveau international.

Communication

Pour le personnel

KPMG souligne l'importance de la sécurité de l'information, d'un comportement conforme à l'éthique, et de la confidentialité client. KPMG dispose d'un code de conduite applicable à tout le personnel et communique régulièrement ses politiques et procédures. Les différents programmes de formation du personnel comprennent des chapitres sur l'éthique, la confidentialité, la sécurité, la gestion de la qualité et des risques, et les pratiques propres à nos professions. Ces politiques, procédures et nos brochures d'information, sont publiées sur le site intranet de KPMG et disponibles pour tout le personnel.

De plus, tous les ans, les employés de KPMG doivent signer une déclaration d'engagement, où chacun s'engage à respecter la confidentialité et le caractère privé des données, vis-à-vis des clients en France ou à l'étranger, et vis-à-vis de toute personne travaillant pour le cabinet.

A leur embauche, les employés de KPMG affirment par écrit qu'ils comprennent les règles professionnelles et les politiques de KPMG, applicables dans le cadre de l'exploitation des informations client confidentielles. Cette affirmation est ensuite renouvelée tous les ans.

Pour plus d'informations

Nous espérons que les informations présentes dans ce document répondent aux éventuelles questions sur les pratiques de KPMG en matière de sécurité.

Pour plus d'informations, veuillez tout d'abord consulter votre manager responsable de l'engagement KPMG. Le cas échéant, vous serez redirigé vers l'équipe responsable de la sécurité de l'information.

Contact

fr-nitso@kpmg.fr

www.kpmg.fr