KPMG

TIME TO ADAPT

COVID-19

Données personnelles : Préserver les droits et libertés fondamentales, en situation de crise

Face à la crise Covid-19 et au confinement qui en découle, l'un des principaux enjeux pour les organisations est d'assurer une continuité des activités, au risque, dans l'urgence, de négliger ou de déprioriser la protection des données personnelles.

On assiste à l'occasion de cette crise, à une explosion des usages numériques, qui impliquent très souvent des traitements de données personnelles de consommateurs comme de salariés. Se profile également, dans un contexte de sortie de crise, l'éventualité de traiter des données de santé des salariés comme des températures corporelles ou l'exposition au virus. Face aux incertitudes sur la durée et les modalités de sortie de crise, les organisations doivent se focaliser sur un niveau minimal de prise en compte des principes de protection des données personnelles dans les traitements réalisés en mode dégradé ou déployés dans l'urgence.

CONTEXTE

L'épidémie de Covid-19 et la mise en place du confinement en France et dans d'autres pays ont fortement impacté la vie des personnes et des organisations : selon un sondage IFOP, **27% des salariés français sont en télétravai**l.

Acteurs privés et publics ont désormais adopté, parfois en urgence, des nouveaux moyens de travail à distance et mettent en place des procédures ad hoc pour assurer la santé des salariés qui ne peuvent pas travailler à distance. Les consommateurs ont massivement recours aux services de e-commerce et les patients privilégient les téléconsultations.

La bascule vers cette nouvelle configuration, le réaménagement des priorités et les opérations en mode dégradé peuvent impliquer **une diminution du niveau de protection des données personnelles.**

Cette situation peut-être illustrée par la polémique autour du manque de transparence de l'usage des données personnelles par des applications de visioconférence, mise en lumière à l'occasion de l'augmentation fulgurante de leur utilisation.

On note également une multiplication des réflexions et initiatives sur des traitements de données personnelles (santé, géolocalisation) et le développement d'outils innovants pour contribuer à la maîtrise de la propagation de l'épidémie. Ces ambitions rencontrent une résistance d'une partie de l'opinion publique qui s'alarme des risques de détournement à des fins illégitimes, de surveillance de masse des populations par exemple.

Aussi, dans un contexte de grande incertitude quant à l'évolution de la crise et aux décisions des autorités**, les organisations ont et auront à faire face à de multiples interrogations en ce qui concerne la protection des données personnelles** : licéité des traitements mis en place dans l'urgence, adaptation des exigences de protection des données personnelles à la situation, sécurisation des données dans un contexte de dématérialisation des usages, etc.

ENJEUX POUR ASSURER LA PROTECTION DES DONNEES

Dans cette situation exceptionnelle, **les organisations doivent relever un double défi : d'une part, continuer ou reprendre leurs activités et, d'autre part,** assurer la santé des personnes, en mettant en œuvre les mesures nécessaires sur le plan sanitaire, tout en respectant leurs droits et libertés fondamentales.

Qu'il s'agisse, dans le contexte de la pandémie, de contrôler des températures corporelles à l'entrée d'un site pour détecter des symptômes du coronavirus, de collecter les données relatives aux déplacements des collaborateurs, ou de mettre en place des moyens de travail à distance, des principes de protection des données personnelles doivent être respectés.

1. Pendant la crise, les organisations doivent définir et mettre en œuvre un cadre minimal de protection des données

- L'enjeu est d'assurer le respect d'un niveau d'exigence « a minima », sur le court terme et adapté au contexte de crise sanitaire. Il s'agit en particulier d'identifier les procédures prioritaires et de les adapter à la crise.

2. Les organisations doivent encadrer les traitements de données personnelles déployés en urgence

- L'enjeu est de maîtriser les risques pour les personnes concernées par les traitements de données mis en œuvre durant la crise, qui peuvent présenter des insuffisances en matière de protection des données du fait d'un déploiement dans l'urgence et en mode dégradé.

3. En sortie de crise, les organisations devront assurer un retour à la normale en réévaluant les traitements et données personnelles, en supprimant les traitements non nécessaires, et en prenant en compte les nouveaux usages numériques

- L'enjeu est de régulariser la situation en réévaluant les processus et les traitements de données. Il faudra aussi s'assurer que la protection des données est pleinement prise en compte dans les projets de transformation numérique accélérés et systématisés après la crise Covid-19.

DES APPROCHES SPECIFIQUES A VOS ENJEUX

Les équipes pluridisciplinaires de KPMG vous accompagnent avec des approches adaptées à votre contexte.

1 METTRE EN ŒUVRE UN CADRE MINIMAL DE PROTECTION DES DONNEES PERSONNELLES PENDANT LA CRISE

Identifier les principales zones de risque au regard de la protection des données personnelles et **mettre en place un cadre minimal de protection à court terme** :

- Inventaire des modalités de mise en œuvre des traitements existants en situation de crise
- Revue des traitements les plus exposés aux risques (données de santé des salariés, géolocalisation, contrôle du travail à distance, etc.)
- Adaptation et renforcement des processus liés aux traitements à risques

Identifier les processus de gestion des données personnelles prioritaires et les adapter au contexte de crise **:**

- Mise en place d'une approche « *Privacy by design* » en mode accéléré
- Adaptation des exigences de sécurité au contexte (télétravail, recours massif au *cloud*, etc.)
- Adaptation du processus de gestion des violations de données au contexte de crise

2 SECURISER LES TRAITEMENTS DE DONNEES PERSONNELLES DEPLOYES EN URGENCE

Mise en conformité de traitements de données induits par la situation de crise (ex. mise en place d'outils collaboratifs, travail à distance, etc.) :

- **Analyse rapide des principales zones de risques** du point de vue de la protection des données personnelles (« Privacy by design ») : vérification du respect des principes de finalité, de proportionnalité, de loyauté et de minimisation ainsi que des mesures de sécurité techniques et organisationnelles en particulier pour les données de santé
- **Sélection et mise en œuvre des actions adaptées** au contexte, au niveau de risque identifié et aux technologies utilisées : information complémentaire des personnes, procédures spécifiques et mesures de sécurité (chiffrements, gestion des accès), etc.

3 ASSURER LA PROTECTION DES DONNEES PERSONNELLES DE MANIERE PERENNE ET ADAPTEE EN SORTIE DE CRISE

Adapter le cadre de protection des données personnelles au contexte de sortie de crise :

- Cartographie exhaustive des traitements de données personnelles mis en place ou modifiés à l'occasion de la crise
- Mise en conformité « a posteriori » des traitements (suppression des données ou des traitements devenus inutiles, ajustement des fonctionnalités, mise à jour de la documentation, etc.), la CNIL n'ayant pas annoncé de tolérance particulière

Intégrer le cadre de protection des données dans la continuité d'activité et la gestion de crise : exploiter les leçons de la crise Covid-19 afin de préparer la protection des données personnelles dans les contextes de crise

Intégrer la protection des données dans la transformation numérique, qui va s'accélérer et se systématiser en sortie de crise : télétravail, espaces collaboratifs, visioconférence, e-commerce, etc.

NOS ATOUTS

- Une capacité prouvée à construire des équipes pluridisciplinaires : Privacy & Cyber, juridique (KPMG Avocats), gestion de projet, conduite du changement, transformation technologique, risques et spécialistes métiers, pour répondre aux demandes complexes de nos clients
- Une capacité à dialoguer avec tous les niveaux d'interlocuteurs dans les organisations, de la Direction générale aux métiers, ainsi qu'au Délégué à la protection des données et à la Direction des systèmes d'information.

Contacts

Vincent MARET
Associé Cyber Sécurité et Protection des données personnelles
Tél. : +33 6 17 12 22 13
Email : vmaret@kpmg.fr

Patrick AMOUZOU
Avocat Associé IP/IT
Tél. : +33 6 21 47 67 54
Email : pamouzou@kpmgavocats.fr

Julie BELLESORT
Avocat Associée IP/IT
Tél. : +33 6 87 21 83 17
Email : jbellesort@kpmgavocats.fr