Déclaration

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Déclaration sur le traitement des données à caractère personnel dans le contexte de l'épidémie de COVID-19

Adoptée le 19 mars 2020

Le comité européen de la protection des données (EDPB) a adopté la déclaration suivante:

Partout en Europe, les gouvernements et les organisations publiques et privées prennent des mesures pour enrayer et atténuer la COVID-19. Ces mesures peuvent impliquer le traitement de différents types de données à caractère personnel.

Les règles en matière de protection des données (telles que le RGPD) n'entravent pas les mesures prises dans le cadre de la lutte contre la pandémie de coronavirus. La lutte contre les maladies transmissibles constitue un important objectif partagé par toutes les nations et il convient donc de la soutenir de la meilleure manière possible. Il est dans l'intérêt de l'humanité de freiner la propagation des maladies et d'utiliser des techniques modernes pour lutter contre les fléaux qui frappent de grandes parties du monde. Malgré tout, l'EDPB souhaite souligner le fait que, même en cette période hors du commun, le responsable du traitement des données et le sous-traitant doivent garantir la protection des données à caractère personnel des personnes concernées. Par conséquent, il y a lieu de tenir compte d'un certain nombre de considérations pour garantir la licéité du traitement des données à caractère personnel et, en tout état de cause, il convient de rappeler que toute mesure prise dans ce contexte doit respecter les principes généraux du droit et ne pas être irréversible. L'urgence est une circonstance juridique susceptible de légitimer des restrictions aux libertés à condition que ces restrictions soient proportionnées et limitées à la période d'urgence.

1. Licéité du traitement

Le **RGPD est un texte législatif de portée générale; il prévoit des règles qui s'appliquent au traitement des données à caractère personnel, y compris dans un contexte tel que celui de la COVID-19**. **Le RGPD permet aux autorités compétentes en matière de santé publique et aux employeurs de traiter des données à caractère personnel dans le contexte d'une épidémie, conformément au droit national et selon les conditions qui y sont fixées**. Il en est ainsi, par exemple, lorsque le traitement

est nécessaire pour des motifs d'intérêt public important dans le domaine de la santé publique. Dans ces circonstances, il n'est pas nécessaire de recueillir le consentement des personnes.

1.1 En ce qui concerne le traitement, par les autorités publiques compétentes (par exemple, les autorités de santé publique)**, de données à caractère personnel, y compris de catégories particulières de données**, l'EDPB considère que les articles 6 et 9 du RGPD permettent le traitement de données à caractère personnel, en particulier lorsque ce traitement relève du mandat légal confié à l'autorité publique par la législation nationale et qu'il respecte les conditions énoncées par le RGPD.

1.2 Dans le contexte de l'emploi, le traitement de données à caractère personnel peut être nécessaire au respect d'obligations légales qui incombent à l'employeur, telles que les obligations relatives à la santé et à la sécurité sur le lieu de travail, ou pour des considérations d'intérêt public, notamment la lutte contre les maladies et d'autres menaces pour la santé. Le RGPD prévoit également des dérogations à l'interdiction du traitement de certaines catégories particulières de données à caractère personnel, notamment de données concernant la santé, lorsque ce traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique [article 9, paragraphe 2, point i)], sur la base du droit de l'Union ou du droit d'un État membre, ou lorsqu'il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée [article 9, paragraphe 2, point c)], le considérant 46 faisant explicitement référence à la lutte contre une épidémie.

1.3 En ce qui concerne le traitement de données relatives aux télécommunications, **telles que les données de localisation**, la législation nationale mettant en œuvre la directive «vie privée et communications électroniques» doit également être respectée. En principe, les données de localisation ne peuvent être utilisées par l'opérateur que de manière anonymisée ou avec le consentement des personnes. Toutefois, l'article 15 de **la directive «vie privée et communications électroniques» permet aux États membres d'adopter des mesures législatives visant à sauvegarder la sécurité nationale.** Une telle législation d'exception n'est possible que **si** elle constitue une **mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique**. Ces mesures doivent être conformes à la charte des droits fondamentaux et à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. En outre, elles sont **soumises au contrôle juridictionnel de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme**. En cas de situation d'urgence, elles devraient également être strictement limitées à la durée de l'urgence en question.

2. Principes fondamentaux relatifs au traitement des données à caractère personnel

Les données à caractère personnel nécessaires pour atteindre les objectifs poursuivis devraient être traitées pour des finalités déterminées et explicites.

En outre, les personnes concernées devraient recevoir des informations transparentes sur les activités de traitement effectuées et leurs principales caractéristiques, y compris la durée de conservation des données récoltées et les finalités du traitement. Les informations fournies devraient être facilement accessibles et formulées en des termes clairs et simples.

Il est important d'adopter des mesures de sécurité et des politiques de confidentialité adéquates garantissant que les données à caractère personnel ne seront pas divulguées à des parties non autorisées. Les mesures mises en œuvre pour gérer l'urgence actuelle devraient être dûment documentées, de même que le processus décisionnel sous-jacent.

3. Utilisation des données de localisation mobile

- **Les gouvernements des États membres peuvent-ils utiliser les données à caractère personnel relatives aux téléphones mobiles des particuliers dans leurs efforts visant à surveiller, enrayer ou atténuer la propagation de la COVID-19?**

Dans certains États membres, les gouvernements envisagent d'utiliser les données de localisation mobile comme moyen possible de surveiller, d'enrayer ou d'atténuer la propagation de la COVID-19. Cela comprendrait, par exemple, la possibilité de géolocaliser des personnes ou de transmettre des messages de santé publique par téléphone ou SMS aux personnes situées dans une zone précise. **Les autorités publiques devraient d'abord s'efforcer de traiter les données de localisation de manière anonymisée (c'est-à-dire sous une forme agrégée qui rend impossible la réidentification des personnes), ce qui pourrait permettre la production de rapports sur la concentration d'appareils mobiles à un endroit donné («cartographie»).**

Les règles en matière de protection des données à caractère personnel ne s'appliquent pas aux données qui ont été adéquatement anonymisées.

Lorsqu'il n'est pas possible de traiter uniquement des données anonymes, la directive «vie privée et communications électroniques» **permet aux États membres d'adopter des mesures législatives pour sauvegarder la sécurité nationale** (article 15).

Si des mesures permettant le traitement de données de localisation non anonymisées sont instaurées, l'État membre est tenu de mettre en place des **garanties appropriées**, notamment en garantissant aux bénéficiaires de services de communication électronique le **droit à un recours juridictionnel**.

Le principe de proportionnalité s'applique également. Il convient toujours de privilégier les solutions les moins intrusives, compte tenu de la finalité particulière à atteindre. Des mesures invasives telles que celles consistant à suivre les déplacements des personnes (c'est-à-dire le traitement de données de localisation historiques non anonymisées) pourraient être considérées comme proportionnées dans des circonstances exceptionnelles et en fonction des modalités concrètes du traitement. Elles devraient cependant faire l'objet d'une surveillance et de garanties renforcées pour assurer le respect des principes de la protection des données (proportionnalité de la mesure en termes de durée et de portée, conservation limitée des données et finalité limitée).

4. Emploi

- **Un employeur peut-il exiger des visiteurs ou des salariés qu'ils fournissent des informations spécifiques en matière de santé dans le contexte de la COVID-19?**

L'application du principe de proportionnalité et de minimisation des données revêt ici une pertinence particulière. L'employeur ne devrait exiger des informations concernant la santé que dans la mesure permise par le droit national.

- **Un employeur est-il autorisé à soumettre ses salariés à des contrôles médicaux?**

La réponse dépend des législations nationales dans le domaine du travail ou de la santé et de la sécurité. Les employeurs ne devraient avoir accès à des données concernant la santé et traiter de telles données que si le respect de leurs propres obligations juridiques l'exige.

- **Un employeur peut-il révéler qu'un salarié est atteint de la COVID-19 à ses collègues ou à des personnes extérieures?**

Les employeurs devraient informer leur personnel des cas de COVID-19 et prendre des mesures de protection mais ne devraient pas communiquer plus d'informations que nécessaire. Dans les cas où il est nécessaire de révéler le nom du ou des salariés ayant contracté le virus (par exemple dans un contexte de prévention) et où le droit national permet de le faire, les salariés concernés devront être informés au préalable, et leur dignité et leur intégrité devront être préservées.

- **Quelles informations traitées dans le contexte de la COVID-19 peuvent être obtenues par les employeurs?**

Les employeurs peuvent obtenir des informations à caractère personnel pour remplir leurs obligations et pour organiser le travail en conformité avec la législation nationale.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)