LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD)

Orientations du CEPD. Réactions des institutions de l'UE, en tant qu'employeurs, à la crise de la COVID-19

15 juillet 2020

Résumé

Les institutions, organes et agences européens ont dû réagir à la crise de la COVID-19 non seulement dans leurs rôles politiques, mais aussi en tant qu'employeurs. Les changements intervenus dans le fonctionnement des institutions, tels que le passage de la grande majorité du personnel au télétravail, ont soulevé de nombreuses questions à propos desquelles les IUE ont consulté le CEPD.

Le présent document rassemble les conseils que nous avons prodigués sur des sujets tels que les outils de télétravail, la gestion du personnel, les aspects liés aux données relatives à la santé et les réponses aux demandes d'accès des personnes concernées.

Le présent document s'appuie sur l'expérience acquise ces derniers mois. Il aborde les questions qui nous ont été soumises et celles que nous avons nous-mêmes rencontrées. Il n'a aujourd'hui rien perdu de son actualité, car le télétravail continuera très probablement à jouer un rôle de premier plan dans la «nouvelle norme» des activités des IUE.

Table des matières

1. Introduction

L'épidémie de COVID-19 a contraint de nombreuses IUE à réorienter leurs activités presque exclusivement vers le télétravail pour la majeure partie de leur personnel. Certaines IUE ont également procédé à d'autres adaptations de leurs activités et prévoient désormais des mesures pour protéger agents et visiteurs à leur retour au bureau. Toutefois, l'urgence de la situation ne doit pas nous faire oublier les règles de protection des données applicables aux IUE. **Les règles de protection des données actuellement en vigueur au sein des IUE sont suffisamment souples pour leur permettre d'adopter diverses mesures en vue de garantir la continuité de leurs opérations, et le CEPD est pleinement conscient qu'il faut parfois du temps pour s'ajuster aux situations d'urgence.** Cela étant dit, il ne doit faire aucun doute que les exigences essentielles en matière de protection des données énoncées à l'article 8 de la charte des droits fondamentaux de l'UE et dans le règlement (UE) 2018/1725 (ci-après le «règlement»), telles que les principes de responsabilité, de protection des données dès la conception et par défaut, de sécurité et de transparence, restent d'application. En tant qu'institutions publiques, les IUE se doivent de montrer l'exemple. Il en va de la confiance que leur personnel, les parties prenantes et le grand public placent en elles.

Bien que les IUE soient déjà en train de planifier un éventuel retour progressif au bureau, le télétravail continuera probablement à jouer un rôle de premier plan dans un avenir proche. Ce document s'appuie sur l'expérience acquise ces derniers mois et aborde les questions qui nous ont été soumises ou que nous avons nous-mêmes rencontrées.

Le présent document s'adresse aux responsables du traitement des données et aux délégués à la protection des données (DPD) des IUE. Les responsables du traitement devraient consulter le DPD de leur IUE très tôt dans le processus d'élaboration des réponses organisationnelles à cette crise. Les DPD guident et conseillent les responsables du traitement, mais en définitive, ce sont ces derniers qui sont responsables de la conformité avec le règlement. Par conséquent, le «vous» dans les pages qui suivent, comme dans «vous devriez faire X», s'adresse aux responsables du traitement.

2. Outils de télétravail

Le besoin d'outils de télétravail pour garantir la continuité des activités s'est considérablement accru sur un laps de temps extrêmement court, notamment pour les conférences téléphoniques, la collaboration à distance, l'audioconférence et la visioconférence ou encore les webinaires. Certaines IUE disposaient déjà des outils nécessaires, tandis que d'autres sont à la recherche de solutions. Si vous avez déjà signé des accords contractuels avec des prestataires externes pour de nouveaux produits et services, au vu de l'urgence de la situation, vous devriez commencer à étudier leurs conditions générales afin de vérifier leur conformité avec le règlement ou déterminer les mesures à prendre pour atténuer les risques de non-conformité.

Compte tenu de la taille du marché et du nombre d'outils disponibles, le CEPD n'est pas en mesure de fournir un «guide de l'acheteur» complet de ces outils. Si vous fournissez ces outils à différentes IUE ou si vous avez rejoint un groupement d'IUE en vue de sélectionner un service ou un logiciel, il vous faudra examiner ces questions au bénéfice de toutes les autres IUE concernées. Des conditions générales particulières basées sur le règlement peuvent ne pas être nécessaires pour autant que des éléments similaires, conformes au règlement 2016/679 (RGPD), puissent déjà répondre à vos besoins (et pour autant qu'ils ne soient pas en

contradiction avec d'autres exigences, supplémentaires ou différentes, énoncées dans le règlement).

Nous pouvons toutefois vous donner quelques conseils sur les problèmes et les pièges les plus courants auxquels il convient d'être attentif et vous aider à choisir des outils respectueux de la protection des données:

2.1 Processus décisionnel

Les besoins opérationnels qui se font jour dans ces circonstances exceptionnelles ne devraient pas amener les IUE à perdre de vue les exigences en matière de protection et de sécurité des données dans leur recherche d'outils de télétravail adéquats. Tenez compte du fait que bien souvent, aucun outil ne répondra à tous vos besoins. Il est donc conseillé aux IUE de définir leurs exigences au moyen de cas d'utilisation (en ce compris les garanties de protection des données) et de rechercher les outils qui y correspondent le mieux.

Bien que la situation actuelle puisse nécessiter des décisions rapides, veillez, **dans la mesure du possible, à suivre les processus de gouvernance informatique établis de votre IUE** tout en restant à l'affût des problèmes de protection des données susceptibles de découler de la mise en œuvre envisagée de ces outils et en y répondant (protection des données dès la conception). Vous devrez associer votre **DPD** à ce processus. Assurez-vous de disposer d'une vue d'ensemble des outils utilisés, d'une évaluation préalable de leurs fonctionnalités de sécurité, de confidentialité et de respect de la vie privée, et faites-vous conseiller par votre service informatique, afin que votre IUE puisse prendre une décision éclairée, de préférence au plus haut niveau hiérarchique.

Dans le cas contraire, il peut y avoir un **risque que certains éléments de votre organisation se mettent à utiliser des outils disponibles gratuitement qui pourraient ne pas être conformes à la stratégie informatique de votre IUE**, exposer des données à caractère personnel ou d'autres informations confidentielles à des tiers ou à des assaillants externes et inutilement exposer votre IUE à des risques de réputation et autres. Ne pas aborder ces questions maintenant peut créer des phénomènes de blocage en aval, introduire des problèmes critiques en matière de protection des données et créer des risques de sécurité supplémentaires.

Pour plus d'informations sur ces processus, veuillez consulter les lignes directrices du CEPD sur la gouvernance informatique et la gestion informatique ainsi que l'avis préliminaire du CEPD sur le respect de la vie privée dès la conception.

2.2 Dispositifs professionnels et personnels

Outre la résolution des problèmes de sécurité informatique, il convient de faire preuve d'une grande prudence s'agissant de la protection des données lorsque des dispositifs personnels sont utilisés pour le télétravail. Il est conseillé, lorsque le personnel utilise des appareils personnels aux fins du télétravail (ordinateurs portables, tablettes, etc.), de consulter votre service informatique afin de déceler les problèmes de sécurité potentiels ou de déterminer les paramètres de configuration spécifiques à appliquer. Si des données à caractère personnel sont appelées à être traitées sur des dispositifs personnels, votre institution devrait **fournir aux utilisateurs des politiques et des instructions claires** sur la façon de traiter ces données (par exemple, sous la forme d'un guide informatique sur le télétravail à destination du personnel). Inversement, la fourniture d'équipements professionnels donnera à votre IUE une plus grande

maîtrise sur l'environnement informatique utilisé par le personnel et réduira la tentation de «basculer du côté obscur de l'informatique».

Par ailleurs, gardez à l'esprit le principe de minimisation des données et évitez de partager inutilement des données personnelles lors de la gestion des demandes d'appareils professionnels dans votre IUE.

Pour plus d'informations sur la gestion des appareils mobiles, qu'il s'agisse d'appareils professionnels ou personnels, veuillez consulter les lignes directrices du CEPD sur les appareils mobiles.

2.3 Rôles du responsable du traitement/sous-traitant

Assurez-vous que tout logiciel/service utilisé ne révèle pas de données à caractère personnel sur vos équipes et ses partenaires de communication au fournisseur/à l'éditeur du logiciel.

Lorsqu'elles font appel à des prestataires externes pour de nouveaux produits ou services, les IUE devraient toujours viser à **privilégier les outils les plus respectueux de la vie privée et à s'assurer qu'elles ont un contrôle approprié sur la manière dont les prestataires externes traiteront les données qui leur sont confiées**. Même si le contrat repose sur des conditions générales communes à tous les clients (c'est par exemple le cas de la plupart des services en ligne), compte tenu du rôle des IUE en tant qu'institutions de service public, il est nécessaire de vérifier les rôles et les contrôles en place. Généralement, une relation responsable du traitement/sous-traitant où votre IUE joue le rôle de responsable du traitement est celle qui offre la plus grande maîtrise à votre IUE. Pour éviter tout problème concernant la responsabilité de l'activité de traitement des données, assurez-vous que les rôles et responsabilités du responsable du traitement et du sous-traitant sont clairement définis. **Assurez-vous également que vos accords responsables du traitement/sous-traitant couvrent tous les éléments obligatoires au titre de l'article 29, paragraphe 3, du règlement**, par exemple disposer de toutes les informations nécessaires concernant les sous-traitants qui sont partie à l'accord de traitement.

Pour plus d'informations, veuillez consulter l'article 29 du règlement et les lignes directrices du CEPD sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement dans le cadre du règlement (UE) 2018/1725.

2.4 Traitement des données dans l'UE/EEE et transferts de données

Si vous devez faire appel à un prestataire externe, vérifiez d'abord si un prestataire établi dans l'UE/EEE satisfait à vos exigences et assurez-vous que votre accord responsable du traitement/sous-traitant est conforme aux exigences énoncées au point 2.3 (voir ci-dessus).

Lorsque vous faites appel à de tels prestataires établis dans l'UE/EEE, veillez à bien vérifier si leurs services impliquent des transferts de données à caractère personnel en dehors de l'UE/EEE, y compris à des fins telles que la sauvegarde, le dépannage/le support client, etc. Si tel est le cas, assurez-vous que votre prestataire dispose de garanties adéquates, répondant aux exigences énoncées au chapitre V du règlement, telles que des règles d'entreprise contraignantes approuvées.

Si le prestataire externe retenu n'est pas établi dans l'UE/EEE et ne relève pas d'une décision d'adéquation de la Commission européenne, il vous faudra obtenir de celui-ci des **garanties appropriées** en vertu de l'article 48 du règlement.

Pour de plus amples informations à ce sujet, veuillez vous reporter à la note d'information du CEPD sur les transferts internationaux de données après le Brexit, qui fournit un aperçu des différents instruments de transfert dont disposent les IUE au-delà de ce contexte spécifique.

2.5 Fonctionnalités de surveillance par l'employeur ou le prestataire

Les outils de collaboration à distance et de vidéoconférence permettent souvent une surveillance accrue du personnel par rapport à une collaboration «hors ligne». Par défaut, **il ne devrait y avoir aucune surveillance de la part de l'employeur ni du prestataire**.

S'agissant du **suivi par le prestataire, vérifiez la description de ses services pour vous assurer qu'il n'y a pas de suivi en place et, si nécessaire, obtenez des garanties contractuelles supplémentaires**.

Concernant le **suivi par l'employeur, configurez les outils de manière à éviter une telle collecte de données et faites preuve de transparence à ce sujet vis-à-vis du personnel**. Si vous avez besoin d'une certaine forme de surveillance «employeur», vous devrez établir si ces mesures intrusives sont proportionnées à l'objectif recherché. Vous pouvez consulter nos lignes directrices sur la proportionnalité sur ces questions et appliquer les obligations de protection des données dès la conception et de protection des données par défaut afin d'atteindre votre objectif tout en respectant le droit à la vie privée de vos équipes. En outre, gardez à l'esprit que le personnel travaille à domicile, parfois avec ses dispositifs personnels. Il ne s'agit pas d'empiéter sur son espace personnel ni sur sa vie privée numérique. Bien que les lignes directrices sur la vidéosurveillance traitent principalement de la vidéosurveillance, vous y trouverez aussi des orientations générales sur la surveillance du personnel en télétravail dans les sections relatives au contrôle des employés (p. 25), aux sites où les personnes s'attendent à un respect plus important de leur vie privée (p. 34) et à la surveillance dissimulée (p. 35).

Dernier point pratique: les outils de vidéoconférence permettent généralement l'enregistrement des réunions. Vous devriez **suivre la même approche pour l'enregistrement que pour les réunions en personne**: cela nécessitera généralement l'obtention du consentement des personnes enregistrées.

2.6 Conservation des données

Qu'ils soient fournis en interne ou par des prestataires externes, assurez-vous que tous les nouveaux outils sont configurés avec des **périodes de conservation appropriées** conformément à l'objectif de l'activité de traitement des données. Pour les **prestataires externes, obtenez un engagement clair et contraignant sur le fait que les informations de votre IUE vous seront retournées ou seront effacées au terme du contrat** [voir également ci-dessus concernant la relation responsable du traitement/sous-traitant – il s'agit d'une exigence contraignante à imposer à vos sous-traitants, en vertu de l'article 29, paragraphe 3, point g), du règlement].

2.7 Sécurité des données

L'adoption de nouveaux outils de télétravail ou l'utilisation accrue des outils existants de télétravail peuvent soulever d'autres problèmes en matière de sécurité des données.

Votre service informatique, en collaboration avec votre responsable local de la sécurité de l'information, doit prendre les mesures qui s'imposent pour protéger la confidentialité, l'intégrité et la disponibilité du traitement des données à caractère personnel effectué par différents moyens de communication électronique: plateformes de messagerie instantanée,

outils de collaboration en ligne, messagerie web, outils de visioconférence, etc. **La sécurité nécessite une collaboration entre les services informatiques, le responsable local de la sécurité de l'information, le DPD et tous les utilisateurs.**

La généralisation du télétravail en guise de réponse à la pandémie de COVID-19 et la charge croissante émanant de connexions externes sur le réseau de l'institution qui l'a accompagnée pourraient conduire **à s'écarter des processus standard** et déboucher sur l'inaccessibilité d'outils automatisés pendant le télétravail. Il existe donc un **risque plus élevé de violations de données à la suite d'une erreur humaine**. Les obligations de signalement des violations de données à caractère personnel demeurent. Les lignes directrices du CEPD sur les notifications de violation de données à caractère personnel fournissent des conseils pratiques à cet égard.

Recensez et documentez les processus «bis» à suivre, assurez-vous que tout votre personnel dispose d'un canal de communication clair avec le responsable local de la sécurité de l'information et **sensibilisez les équipes aux sources courantes de violation de données telles que l'augmentation des phénomènes d'usurpation, des tentatives d'hameçonnage ou encore des attaques d'ingénierie sociale reposant sur des messages liés à la COVID-19**. Plusieurs rapports font également état d'outils de conférence en ligne ciblés, où des pirates informatiques ont obtenu un accès non autorisé à des conversations et ont envoyé des courriers électroniques d'hameçonnage pour tenter de dérober des identifiants.

S'agissant des nouveaux outils, les exigences générales en matière de sécurité des données prévues à l'article 33 du règlement et les autres obligations liées à la sécurité de l'information restent d'application. Ainsi, les technologies fondées sur les meilleures pratiques en matière de cryptographie devraient être utilisées selon une approche fondée sur les risques afin d'assurer le chiffrement de bout en bout (par opposition au chiffrement point à point), l'authenticité de l'expéditeur et l'intégrité de l'information.

Les nouveaux contrats et accords sur les niveaux de service avec des prestataires de services externes fournissant des services informatiques devraient être examinés afin de s'assurer qu'ils mettent en œuvre des mesures de sécurité suffisantes.

Ce serait également l'occasion de vérifier si les outils existants satisfont à toutes les exigences énoncées ci-dessus et de mettre à jour vos politiques actuelles, telles que la politique en matière de sécurité.

Les lignes directrices du CEPD sur l'utilisation des services d'informatique en nuage par les institutions et organes de l'Union européenne sont toujours pertinentes à cet égard. Vous pouvez également consulter les lignes directrices du CEPD sur les applications mobiles. Bien que ces documents fournissent des conseils aux IUE qui développent leurs propres applications, les questions soulevées sont également pertinentes pour les fournisseurs d'applications auxquels votre IUE pourrait commencer à avoir recours.

3. Questions concernant les données relatives à la santé

3.1 Rôle des services médicaux

En règle générale, l'accès aux données relatives à la santé et leur traitement sont limités aux professionnels de la santé qualifiés.

Votre service médical est bien placé pour fournir des conseils sur les mesures préventives à l'interne. Les agents (soupçonnés d'être) contaminés par la COVID-19 doivent coopérer avec

leur prestataire de soins, les autorités nationales compétentes (en matière de santé publique) et le service médical de leur IUE, le cas échéant.

Suivre l'évolution du cas clinique est d'abord la tâche du médecin traitant de la personne concernée. Néanmoins, le service médical de votre IUE sera impliqué si nécessaire, comme pour tout congé de maladie.

Les IUE devront néanmoins veiller au respect du secret médical de leur personnel et aux exigences supplémentaires énoncées à l'article 10 du règlement pour tout ce qui touche au traitement de données relatives à la santé. Néanmoins, compte tenu du taux élevé de contagion de la COVID-19 et de l'obligation de diligence des IUE envers leur personnel, les services médicaux des IUE pourront adopter des mesures de suivi supplémentaires pour les cas suspects ou confirmés.

Si une autre IUE vous fournit des services médicaux en vertu d'un SLA ou accord analogue, le même principe s'applique. Il peut être judicieux d'envoyer un rappel au service médical qui fournit ces services à votre IUE.

Comme l'a déjà indiqué le CEPD, cette crise pourrait nécessiter des mesures temporaires et, par conséquent, tout stockage de données supplémentaires liées à cette crise devrait également être temporaire. Il est de bonne pratique d'aborder cette question à un stade précoce et de décider de déclencher la suppression de ces données après qu'un jalon de santé publique défini a été atteint dans la crise.

3.2 Notification d'exposition et suivi des contacts

Le suivi des contacts est l'un des outils à la disposition des autorités de santé publique pour endiguer les maladies infectieuses.

Comme cela a déjà été expliqué dans des orientations précédentes[1], **si les autorités de santé publique compétentes contactent les IUE dans le cadre de leurs activités nationales de suivi des contacts, les IUE peuvent divulguer des informations pertinentes** (par exemple, les personnes qui ont assisté à une même réunion, qui partagent des bureaux, etc.) tout en préservant le secret médical de ces informations, comme expliqué à la section 3.1. Qu'advient-il des données communiquées aux autorités sanitaires nationales compétentes? Celles-ci doivent les traiter conformément à la législation applicable.

Dans certains États membres de l'UE, la COVID-19 est une maladie transmissible à déclaration obligatoire, de sorte que le médecin généraliste qui a posé le diagnostic signalera tout cas positif aux autorités sanitaires (y compris le nom de la personne, et l'autorité sanitaire prendra contact avec elle afin d'assurer le suivi de ses contacts). Informer ses collègues de l'identité d'un cas confirmé: lors du suivi de contacts «de la vieille école», les autorités sanitaires veillent à ne pas divulguer ces informations.

Cela signifie que le RGPD et les actes juridiques qui confient ces tâches aux autorités nationales compétentes s'appliquent à leur traitement ultérieur. Les autorités compétentes sont ici des responsables du traitement distincts des institutions européennes. Les délais de conservation, les droits des personnes concernées, etc., suivent les procédures adoptées par les autorités compétentes. L'APD nationale compétente supervise leur conformité au RGPD.

[1] Message à tous les DPD des IUE du 12 mars 2020

3.3 Aspects sociaux et privés

Les IUE ne doivent pas divulguer l'identité des cas confirmés au personnel en général. Cela étant dit, si un membre du personnel mentionne délibérément son propre état de santé à ses collègues, les règles de protection des données **n'empêchent pas les initiatives sociales organisées entre collègues pour, par exemple, envoyer des fleurs ou une carte aux malades**.

4. Droits des personnes concernées

La crise du coronavirus **ne suspend pas non plus les droits des personnes concernées, et celles-ci sont habilitées à exercer leurs droits**, à moins que des restrictions spécifiques, dûment adoptées et documentées au titre de l'article 25 du règlement ne s'appliquent.

Assurez-vous d'avoir un accès à distance aux systèmes d'information pour les demandes d'accès. Si vous êtes toujours confronté(e) à une situation dans laquelle votre IUE ne sera pas en mesure de répondre en temps opportun aux demandes, vous devez documenter les raisons sous-jacentes et la prise de décision, et communiquer aux personnes concernées, avant l'expiration du délai légal, qu'il y aura un retard dans la réponse à leurs demandes, la raison de celui-ci et la durée prévue du retard.

5. Le CEPD assiste les IUE

Durant la crise actuelle, il est essentiel de se conformer aux exigences énoncées dans le règlement et dans la charte des droits fondamentaux. Ainsi, assurez-vous de régulièrement mettre à jour votre registre des opérations de traitement et d'effectuer toutes les AIPD nécessaires. En vertu du principe de responsabilité, il devrait y avoir une trace permettant de documenter les décisions prises en matière de protection des données.

Le CEPD est conscient que toutes les IUE traversent actuellement une période difficile. Comme indiqué précédemment, et comme le montre le présent document, le règlement reste d'application et il est suffisamment souple pour être adapté à l'environnement actuel.

Lorsque la crise s'estompera (ou en réaction aux éventuelles plaintes reçues), le CEPD peut réexaminer les mesures prises par votre institution au cours de cette crise en matière de protection des données.

Nous restons à votre disposition pour vous aider et vous fournir des conseils spécifiques, formels et informels, sur toute question liée à cette crise.