## Document public du CEPD sur

# Résultats de l'enquête d'initiative sur l'utilisation des produits et des services Microsoft par les institutions de l'UE

2 juillet 2020

Le contrôleur européen de la protection des données (CEPD) est l'autorité de contrôle indépendante instituée par l'article 52 du règlement (UE) 2018/1725 qui est compétente pour:

- contrôler et assurer l'application des dispositions du règlement (UE) 2018/1725 et de tout autre acte de l'Union relatif à la protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union;
- conseiller les institutions et organes de l'UE et les personnes concernées sur toutes les questions relatives au traitement des données à caractère personnel.

À cette fin, le CEPD remplit ses fonctions conformément à l'article 57 du règlement (UE) 2018/1725 et exerce les pouvoirs qui lui sont conférés par l'article 58 de ce même règlement.

Le pouvoir d'enquête est l'un des outils mis en place pour contrôler et garantir le respect du règlement (UE) 2018/1725.

Le présent document expose les questions soulevées par l'enquête d'initiative du CEPD sur l'utilisation des produits et services Microsoft par les institutions, organes et organismes européens (ci-après les «institutions de l'UE»). Ces conclusions et recommandations issues de l'enquête sont susceptibles de présenter un intérêt non seulement pour les institutions de

l'UE, mais plus largement pour toutes les autorités publiques des États membres de l'UE/EEE.

Le CEPD a évalué la conformité de l'accord de licence entre Microsoft et les institutions de l'UE avec les exigences énoncées dans le règlement (UE) 2018/1725[1], qui définit les règles relatives à la protection des données dans les institutions, organes et organismes de l'UE, ainsi que les missions et compétences du contrôleur européen de la protection des données (CEPD).

Dans l'intérêt d'une approche cohérente de la protection des données à caractère personnel dans l'ensemble de l'Union et de la libre circulation de ces données au sein de l'Union, les législateurs ont aligné, dans la mesure du possible, le règlement (UE) 2018/1725 sur les règles en matière de protection des données énoncées dans le règlement (UE) 2016/679[2] («règlement général sur la protection des données»; ci-après le «RGPD»). Chaque fois que les dispositions du règlement (UE) 2018/1725 suivent les mêmes principes que celles du RGPD, ces deux ensembles de dispositions devraient, conformément à la jurisprudence de la Cour de justice de l'Union européenne, être interprétés de manière homogène, notamment en raison du fait que le régime de ce règlement devrait être compris comme étant équivalent au régime du RGPD.

Le CEPD a formulé les principales conclusions suivantes dans son enquête sur l'utilisation des produits et services Microsoft par les institutions de l'UE.

Premièrement, l'accord de licence entre Microsoft et les institutions de l'UE a permis à Microsoft de définir et de modifier les paramètres de ses activités de traitement effectuées pour le compte des institutions de l'UE et les obligations contractuelles en matière de protection des données. Le pouvoir discrétionnaire dont Microsoft disposait constituait un droit étendu à agir en tant que responsable du traitement. Compte tenu du rôle des institutions de l'UE en tant qu'institutions de service public, le CEPD n'a pas jugé cette situation judicieuse. Le CEPD a recommandé aux institutions de l'UE de prendre des mesures afin de conserver leur rôle de responsable du traitement.

Deuxièmement, les institutions de l'UE avaient besoin de mettre en place un accord entre le responsable du traitement et le sous-traitant qui soit

conforme et complet ainsi que des instructions documentées des institutions de l'UE à l'intention des sous-traitants. Leur manque de contrôle sur les sous-traitants ultérieurs que Microsoft utilisait et l'absence de droits d'audit significatifs posaient également des problèmes importants. Le CEPD a formulé des recommandations sur la manière d'améliorer l'accord entre le responsable du traitement et le sous-traitant et a mis en place des contrôles d'audit solides.

Troisièmement, les institutions de l'UE ont été confrontées à un certain nombre de questions liées concernant la localisation des données, les transferts internationaux et le risque de divulgation illicite de données. Elles n'étaient pas en mesure de contrôler la localisation d'une grande partie des données traitées par Microsoft. Elles n'ont pas non plus correctement contrôlé ce qui était transféré hors de l'UE/EEE ni de quelle manière se faisait le transfert. Les garanties adéquates faisaient aussi défaut pour la protection des données quittant l'UE/EEE. Les institutions de l'UE disposaient par ailleurs de peu de garanties pour défendre leurs privilèges et immunités et veiller à ce que Microsoft ne divulgue les données à caractère personnel que dans la mesure permise par le droit de l'UE. Le CEPD a formulé des recommandations afin d'aider les institutions de l'UE à s'attaquer à ces problèmes.

Quatrièmement, le CEPD a examiné les mesures techniques mises en place par la Commission pour endiguer le flux de données à caractère personnel généré par les produits et services Microsoft et envoyé à cette société. Le CEPD a recommandé à toutes les institutions de l'UE d'effectuer des essais en utilisant une approche révisée et globale, de partager entre elles les connaissances et les solutions techniques qu'elles ont mises au point pour empêcher que des flux non autorisés de données n'arrivent chez Microsoft et de s'informer mutuellement de toutes les questions liées à la protection des données qu'elles relèvent avec les produits ou services.

Cinquièmement, les institutions de l'UE n'avaient pas une vision suffisamment claire de la nature, de la portée et des finalités du traitement ni des risques pour les personnes concernées pour pouvoir s'acquitter de leurs obligations de transparence à l'égard de ces personnes. Le CEPD a recommandé que les institutions de l'UE recherchent la clarté et les garanties leur permettant de tenir les personnes concernées correctement informées.

# Table des matières



# 1 Introduction

## 1.1 Contexte

Le présent document expose les questions soulevées par l'enquête d'initiative du CEPD sur l'utilisation des produits et services Microsoft par les institutions, organes et organismes européens (ci-après les «institutions de l'UE»). Il présente les conclusions et les recommandations du CEPD découlant de l'enquête à partager avec un public plus large, en appliquant un niveau élevé de transparence[3], tout en préservant la nécessaire confidentialité de certains éléments du contrat souscrit par les institutions de l'UE et de l'enquête du CEPD.

Les institutions de l'UE traitent une grande quantité de données à caractère personnel grâce à des produits et services Microsoft. Plus de 45 000 membres du personnel des institutions de l'UE, y compris le CEPD, sont des utilisateurs de ces produits et services. En outre, le personnel utilise des produits et services Microsoft pour traiter les données à caractère personnel de personnes qui ne font pas partie du personnel.

L'enquête du CEPD s'est concentrée sur les termes de l'*accord interinstitutionnel de licence* (ci-après l'«ILA») que les institutions de l'UE ont signé avec Microsoft en 2018. Le CEPD a également examiné les mesures techniques que la Commission européenne, en tant que plus grande institution de l'UE chargée d'une grande variété de tâches, avait mises en œuvre et qui visaient les flux de données à caractère personnel dirigés vers Microsoft.

Le CEPD a publié ses conclusions et ses recommandations aux institutions de l'UE après la clôture de son enquête en mars 2020. Le rapport du CEPD avait pour but de fournir aux institutions de l'UE une assistance prospective dans la mise en conformité de leurs dispositions avec la législation sur la protection des données. En particulier, les conclusions et recommandations du CEPD visaient à soutenir la renégociation de l'ILA et du contrat des institutions de l'UE ainsi qu'à mettre en œuvre les mesures techniques et organisationnelles solides qui devraient accompagner le contrat.

Le traitement par les institutions de l'UE des données à caractère personnel et les compétences de surveillance et d'enquête du CEPD sont régis par le règlement (UE) 2018/1725[4]. Le CEPD a évalué la conformité de l'ILA avec les exigences énoncées dans ce règlement. Bien que le

règlement (UE) 2018/1725 soit un régime de protection des données adapté aux institutions de l'UE et distinct du règlement général sur la protection des données[5] (le «RGPD») mieux connu, le chevauchement entre les dispositions du règlement (UE) 2018/1725 et celles du règlement général sur la protection des données est conséquent.

En conséquence, les conclusions et les recommandations du CEPD sont susceptibles de présenter un intérêt plus large que pour les seules institutions de l'UE[6]. Non seulement la législation appliquée par le CEPD dans son enquête est fondée sur les mêmes principes et partage la grande majorité de ses dispositions avec le RGPD, mais l'accord signé par les institutions de l'UE repose sur des documents types de Microsoft relatifs aux licences en volume et est donc susceptible de présenter des similitudes avec les accords conclus par d'autres organisations. Les conclusions et recommandations du CEPD peuvent présenter un intérêt particulier pour les autorités publiques des États membres de l'UE.

Elles sont probablement aussi pertinentes au-delà de la conclusion et de la mise en œuvre des accords de licence en volume pour les produits et services de Microsoft. Selon le CEPD, les organisations qui externalisent la fourniture ou l'exploitation de services numériques vers d'autres prestataires de services risquent de rencontrer des problèmes similaires.

## 1.2 Recommandations d'ordre général

Le CEPD a recommandé que les institutions de l'UE réfléchissent avec prudence à tout achat de produits et services de Microsoft ou à toute nouvelle utilisation de produits et services existants tant qu'elles n'ont pas analysé et mis en œuvre les recommandations qu'il préconise. Elles devraient solliciter la participation de leurs délégués à la protection des données lorsqu'elles décident de la manière de mettre en œuvre les recommandations du CEPD. Les institutions de l'UE devraient dûment intégrer la protection des données dans chaque procédure de passation de marché public spécifique en matière de technologies de l'information et de la communication, en précisant les mesures de sécurité et de protection des données à mettre en œuvre en ce qui concerne les produits et services particuliers faisant l'objet de la passation de marché.

Cela aidera d'emblée les institutions de l'UE à acquérir des produits et des services pour lesquels les mesures contractuelles et d'autres mesures techniques, organisationnelles et de sécurité sont appropriées, de manière à ce que le traitement des données à caractère personnel par l'intermédiaire de ces outils soit conforme au règlement (UE) 2018/1725, en particulier aux principes de protection des données dès la conception et de protection des données par défaut[7].

## 1.3 L'accord de licence interinstitutionnel (ILA)

L'ILA examiné par le CEPD avait une structure complexe avec une multiplicité de documents interdépendants se complétant et se modifiant mutuellement de différentes manières.

Toutefois, dans les grandes lignes, l'ILA comportait trois volets principaux. Le premier est un accord-cadre, fondé sur un certain nombre de documents types de licence en volume pour lesquels les institutions de l'UE ont négocié un ensemble de modifications sur mesure avec Microsoft. Le deuxième volet comprend plusieurs séries de conditions types de Microsoft, qui ont été intégrées dans l'accord-cadre par référence. Dans le cadre de l'enquête du CEPD, les ensembles de conditions types les plus importants étaient les *conditions relatives aux produits* et les *conditions relatives aux services en ligne*. Le troisième volet comprend les documents par lesquels les différentes institutions de l'UE ont adhéré à l'accord de licence et ont souscrit à un ensemble de produits et de services de Microsoft répondant le mieux à leurs besoins.

Les conditions prévues à l'ILA n'étaient pas définitives. Les ensembles de conditions types de Microsoft qui ont été intégrées dans l'accord-cadre sont modifiées régulièrement par Microsoft, de nouvelles versions étant publiées sur son site web relatif aux licences en volume[8]. Par exemple, Microsoft publie tous les mois une nouvelle version de ses conditions relatives aux services en ligne.

Cela peut être une entreprise complexe que de déterminer quelles parties de quelle version d'un document type concernent tel ou tel aspect d'un produit ou d'un service donné de Microsoft. Pour reprendre l'exemple des conditions relatives aux services en ligne, la version applicable de ce document a varié, pour chaque service en ligne, en fonction de la date à laquelle le client

concerné a acheté pour la première fois ou renouvelé un abonnement à ce service[9]. Toutefois, les conditions introduites dans les versions ultérieures des conditions relatives aux services en ligne pouvaient également s'appliquer à de nouvelles fonctionnalités et aux compléments de logiciels connexes qui ne figuraient pas précédemment dans l'abonnement[10].

Dans le cadre de l'enquête réalisée par le CEPD, la dernière version des documents types qu'il a analysée était celle de janvier 2020[11]. Aux fins du présent document, le CEPD ne fait référence qu'à cette version. Au cours de l'enquête, cependant, le CEPD a également analysé un certain nombre de versions antérieures[12], qui étaient souvent rédigées dans des termes similaires et présentaient des problèmes comparables ou plus importants de conformité aux dispositions. Dans l'ensemble, les constatations faites par le CEPD à propos de l'ILA, des documents non contractuels et du contexte factuel traduisent sa position jusqu'en mars 2020.

# 2 Microsoft en tant que responsable du traitement

Selon le CEPD, la portée et les conditions énoncées dans l'ILA ont abouti à ce que Microsoft intervienne en tant que responsable du traitement selon des méthodes qui n'étaient pas transparentes. Cela s'explique par la combinaison de plusieurs aspects de l'ILA. Le CEPD examine trois points essentiels à cet égard:

1. le droit de Microsoft d'apporter unilatéralement une modification;
2. le champ d'application limité des obligations en matière de protection des données dans l'ILA; et
3. l'absence de finalités spécifiques et expressément définies pour le traitement qui intervenait en vertu de cet accord.

## 2.1 Droit d'apporter unilatéralement une modification

L'ILA a permis à Microsoft de modifier unilatéralement les conditions relatives à la protection des données. Ce droit comportait deux aspects.

Premièrement, l'ILA conférait à Microsoft un droit illimité de modifier tous les ensembles de conditions types qui y avaient été incorporés par référence.

Microsoft a pu modifier radicalement les conditions prévues dans l'ILA concernant la protection des données en amendant un ensemble de conditions types qui y sont incorporées. La raison en est que les conditions types comblaient de nombreuses lacunes des accords-cadres négociés, de sorte qu'il était souvent nécessaire de se référer à ces conditions pour comprendre comment celles contenues dans les accords-cadres seraient mises en œuvre.

Les modifications apportées par Microsoft en janvier 2020 illustrent à quel point de telles modifications unilatérales peuvent être radicales. Microsoft a repris plusieurs conditions importantes en matière de protection des données présentes dans les conditions relatives aux services en ligne et les a introduites dans un nouveau document type, dénommé «addendum sur la protection des données». Le contenu de ces conditions relatives à la protection des données a également fait l'objet d'une révision substantielle.

À la suite de cette modification, il est devenu difficile de déterminer si un grand nombre de conditions relatives à la protection des données s'appliquaient encore à l'utilisation que les institutions de l'UE avaient des produits et des services de Microsoft. Étant donné que l'addendum sur la protection des données n'existait pas au moment de la signature de l'ILA en 2018, seules les conditions relatives aux services en ligne ont été intégrées par référence dans l'ILA, mais pas ce nouvel addendum distinct sur la protection des données. Au moment où le CEPD concluait son enquête, il n'existait pas non plus de lien contractuel explicite entre l'addendum sur la protection des données et l'ILA, par exemple une déclaration figurant dans les conditions relatives aux services en ligne selon laquelle l'addendum sur la protection des données ferait partie de ces conditions. Aux fins de son enquête d'initiative, le CEPD a supposé que l'addendum sur la protection des données s'appliquait effectivement dans le contexte de l'ILA.

Le second aspect du droit de modification unilatérale de Microsoft concernait la hiérarchie des différents documents contractuels. L'ILA contient un certain nombre de dispositions indiquant quels documents l'emportent. Certaines de ces dispositions étaient directement en conflit entre elles, ce qui nous a amené à conclure que la hiérarchie exacte des documents était

ambiguë. Néanmoins, de l'avis du CEPD, un risque élevé demeurait que des documents types, tels que les conditions relatives aux services en ligne, les conditions relatives aux produits et potentiellement l'addendum sur la protection des données, l'emportent sur les conditions négociées de l'accord-cadre. Compte tenu du droit de Microsoft de modifier à tout moment ces documents types, cela représentait un risque élevé que Microsoft puisse modifier unilatéralement l'ensemble de la suite contractuelle de l'ILA, y compris tout accord entre le responsable du traitement et le sous-traitant conclu entre les parties.

D'une manière générale, le CEPD a estimé qu'il existait un risque élevé que la société Microsoft puisse modifier, par exemple, les finalités pour lesquelles elle traitait des données à caractère personnel, la localisation des données et les règles concernant leur divulgation et leur transfert, sans aucun recours contractuel par les institutions de l'UE contre ces modifications. Microsoft détenait le pouvoir discrétionnaire de procéder ou non à de telles modifications.

Ce pouvoir discrétionnaire va au-delà de ce qui peut être confié à un sous-traitant; il faisait de facto de Microsoft un responsable du traitement[13].

## 2.2 Obligations limitées en matière de protection des données

Le champ d'application des principales obligations de Microsoft en matière de protection des données dans les documents négociés de l'ILA était limité à certains types de traitements et catégories de données. Il existait un risque que certaines activités de traitement de données réalisées au titre de l'ILA ne tombent pas dans le champ d'application des conditions négociées et bénéficient d'un niveau de protection inférieur déterminé par Microsoft uniquement. Certaines catégories de données collectées et exploitées par Microsoft suite à l'utilisation par les institutions de l'UE de ses produits et services se situaient purement et simplement hors du cadre des protections contractuelles.

L'analyse faite par le CEPD suggère que, d'une manière générale, quatre catégories de données à caractère personnel bénéficiaient de différents niveaux de protection au titre de l'ILA. La première catégorie de

données à caractère personnel, la plus protégée, est celle des données *fournies* par l'utilisation de *services en ligne*. Les services en ligne étaient, en substance, les services hébergés par Microsoft fournis dans le cadre de l'ILA et comprenaient la composante en ligne de produits logiciels Microsoft. Les données appartenant à cette catégorie relevaient du champ d'application des principales obligations négociées en matière de protection des données dans l'ILA et de l'addendum sur la protection des données.

Une deuxième catégorie comprenait des données qui n'étaient pas *fournies* à la société Microsoft mais *recueillies* par elle lorsque les institutions de l'UE utilisaient les services en ligne. Le traitement de ces données était en partie couvert par les conditions relatives aux services en ligne (et potentiellement, depuis sa création, par l'addendum sur la protection des données) et non par les principales obligations négociées figurant dans l'accord-cadre.

Une troisième catégorie de données consiste en celles que Microsoft obtenait lorsque les institutions de l'UE utilisaient ses *services professionnels*. Cette catégorie a fait l'objet d'un ensemble distinct et allégé de clauses relatives à la protection des données, annexé à l'addendum sur la protection des données. Elle sortait également du cadre des principales obligations négociées figurant dans l'accord-cadre.

Microsoft a traité les données des trois premières catégories non seulement en tant que sous-traitant mais aussi en tant que responsable du traitement[14]. Lorsque Microsoft intervenait en tant que responsable du traitement, sa déclaration de confidentialité s'appliquait en plus des documents contractuels.

Il existait une quatrième catégorie de données. Celles-ci étaient tant *fournies* à la société Microsoft que *recueillies* par elle lorsque les institutions de l'UE utilisaient des produits et des logiciels que Microsoft ne considérait *pas* comme des services en ligne. Le traitement des données de cette catégorie se situait hors du cadre du moindre contrôle contractuel sérieux. Les données étaient traitées par Microsoft en tant que responsable du traitement et couvertes par sa déclaration de confidentialité. Les données diagnostiques de toutes les versions de Windows et de la suite bureautique Microsoft Office (y compris *Office 2016*) relevaient de cette catégorie. Les données diagnostiques provenant des applications de la suite bureautique *Office 365*

*ProPlus* (par exemple Word, Excel, PowerPoint), qui n'étaient pas des services en ligne, relevaient aussi potentiellement de cette catégorie.

Dans l'ensemble, il y avait un manque de transparence sur le point de savoir quels contrôles contractuels, le cas échéant, s'appliquaient aux différentes catégories de données traitées par Microsoft dans le cadre de l'ILA. Le CEPD n'était pas en mesure de délimiter précisément les différentes catégories en se fondant sur les documents contractuels.

Étant donné la nature interconnectée des produits, des services en ligne et des services professionnels de Microsoft, il n'apparaissait pas non plus clairement s'il était possible que les données relevant de la catégorie la plus protégée migrent dans une catégorie moins protégée, ou inversement.

Selon le CEPD, les institutions de l'UE avaient peu ou pas de contrôle contractuel sur les données à caractère personnel collectées par Microsoft auprès des utilisateurs ou sur ce que Microsoft pouvait faire avec ces données, à moins qu'elles n'aient été fournies par l'intermédiaire de services en ligne et qu'il soit certain qu'elles resteraient dans cette catégorie. Comme indiqué dans la section précédente, Microsoft gardait également le droit de modifier unilatéralement de nombreuses restrictions ou potentiellement toutes. Microsoft conservait donc un large pouvoir discrétionnaire à cet égard.

Lorsque le champ d'application des obligations d'un sous-traitant en matière de protection des données ne ressort pas clairement, cela peut créer un risque que ce sous-traitant décide d'agir comme un responsable du traitement pour une partie de toutes les données qu'il traite du fait de la relation commerciale. Dans le cas de l'ILA, le manque de clarté concernant le champ d'application des obligations de la société Microsoft en matière de protection des données nous a amené à constater l'existence d'un risque élevé qu'elle puisse agir en tant que responsable du traitement pour toutes les données traitées au titre de l'ILA.

## 2.3 Limitation insuffisante de la finalité

Le CEPD estime que la limitation de la finalité dans l'ILA n'était pas suffisamment précise ni explicite. Cela a créé un risque d'inadéquation entre la limitation de la finalité que les institutions de l'UE estimaient avoir imposée

à Microsoft dans le cadre de l'ILA et le traitement que cette société considérait comme autorisé en vertu de cet accord.

La formulation la plus explicite dans les documents de l'ILA relative à la finalité des activités de Microsoft en tant que sous-traitant était de «fournir des produits ou des services professionnels». La gamme de traitements que cela pouvait comprendre était potentiellement vaste.

Dans le contexte d'un accord complexe et détaillé, tel que l'ILA, entre opérateurs avertis intéressant un grand nombre de personnes concernées, il importe que les finalités autorisées pour le traitement des données soient spécifiées pour que ne subsiste aucun doute quant à ce qui est et n'est pas inclus dans la finalité[15]. La description devrait également être exhaustive, permettant aux autorités clientes et aux autorités de contrôle de comprendre les risques liés au traitement et de donner l'explication de ces risques aux personnes concernées. Le CEPD estime que la formulation de la finalité figurant dans l'ILA laisse trop de place à l'interprétation.

L'addendum sur la protection des données a permis de clarifier quelque peu ce qui pourrait et ne pourrait pas relever de la «fourniture» d'un service. Il a défini ce que recouvrait l'expression «fournir» un service en ligne ou professionnel, a créé une liste de finalités interdites, à moins que le client n'en dispose autrement, et a explicitement reconnu une série de finalités lorsque Microsoft entendait agir en qualité de responsable du traitement. Sa publication en janvier 2020 a représenté une réorientation importante vers une plus grande transparence dans la documentation contractuelle des opérations de traitement de Microsoft et a donc été la bienvenue.

Cela n'était cependant pas le mot de la fin: ainsi qu'il a été expliqué, l'addendum ne couvrait pas une grande partie du traitement. Il était également difficile de savoir s'il s'appliquait ou non dans le contexte de l'ILA.

En outre, un certain nombre de difficultés subsistaient en lien avec la précision de la limitation de la finalité. Par exemple, l'addendum relatif à la protection des données comportait la mention «fournir des expériences utilisateur personnalisées» dans le cadre de la définition de ce que signifiait «fournir» un service en ligne[16]. Cela était en contradiction directe avec l'interdiction par défaut du «profilage des utilisateurs»[17], soulevant une

question sur l'étroitesse de l'interprétation que donne Microsoft du «profilage des utilisateurs».

La «fourniture d'un service en ligne» a également été définie en des termes assez vagues pour laisser les questions suivantes sans réponse[18]. Premièrement, la définition était suffisamment vaste pour inclure l'analyse des données. Il était donc difficile de savoir si le traitement à des fins telles que les systèmes de formation automatique ou d'intelligence artificielle était autorisé. Deuxièmement, il était difficile de déterminer si la fourniture d'un service en ligne ou professionnel donné ne comprenait que le «dépannage», la «fourniture de capacités fonctionnelles» et l'«amélioration continue» concernant ce service ou également concernant d'autres services ou tous les services en ligne ou professionnels respectivement. Troisièmement, l'«amélioration continue» d'un service a été décrite comme incluant «l'amélioration de la productivité des utilisateurs» et de son «efficacité». La productivité et l'efficacité n'étaient pas clairement définies.

Un autre exemple de l'imprécision en matière de limitation de la finalité prévalant dans l'addendum sur la protection des données était l'interdiction par défaut qu'il imposait pour le traitement «à des fins de publicité ou à des fins commerciales similaires»[19]. Ces termes n'étaient pas expliqués. Cela était significatif, puisque la société Microsoft avait indiqué en 2018 qu'elle considérait que le fait de présenter aux clients des recommandations internes aux applications ciblées pour des produits qu'ils n'utilisent pas ou auxquels ils ne s'abonnent pas ne relevait pas de la publicité ou d'une finalité commerciale similaire[20]. Si Microsoft maintient cette interprétation, elle pourrait considérer que ce traitement s'inscrit dans la finalité autorisée.

L'addendum sur la protection des données a également accordé à Microsoft le droit d'agir en tant que responsable du traitement en ce qui concerne ses «besoins professionnels légitimes», qui étaient définis de manière à couvrir six finalités[21]. La nature déclarée des six finalités suggérait un chevauchement important avec ce qui pourrait être considéré en vertu du RGPD comme étant des intérêts légitimes poursuivis par le responsable du traitement. Il était difficile de comprendre, à partir de la formulation large et vague, dans quelle mesure ces finalités étaient nécessaires à la fourniture des services en ligne et des services professionnels. À tout le moins, on pouvait se demander en quoi des données à caractère personnel provenant des institutions de l'UE pourraient être nécessaires pour décider de primes

destinées au personnel de Microsoft. Comme expliqué dans la sous-section suivante, le CEPD a estimé que le traitement effectué par Microsoft en tant que responsable du traitement, en particulier pour ses propres intérêts légitimes, n'était pas approprié dans le contexte de l'utilisation qu'ont les institutions de l'UE des produits et services de Microsoft dans le cadre de l'ILA.

## 2.4 Conséquences

Selon le CEPD, l'un des aspects les plus inquiétants de l'ILA est que le degré de pouvoir discrétionnaire accordé à Microsoft était largement implicite: l'analyse du CEPD se fondait en grande partie sur la constatation de lacunes dans la formulation contractuelle et sur les conséquences découlant du fait de laisser des lacunes ou des incertitudes dans ce contexte particulier.

Le CEPD est parvenu à la conclusion que l'ILA a accordé à Microsoft des droits étendus en matière de modification unilatérale, en dépit d'une disposition expresse contraire dans les documents négociés. L'analyse par le CEPD du pouvoir discrétionnaire accordé à Microsoft du fait de limitations portant sur le champ d'application de certaines conditions contractuelles repose sur l'énumération des types de traitement qui pourraient *ne pas* être couverts, en tout ou en partie.

L'élément moteur des préoccupations du CEPD en ce qui concerne les limitations de la finalité dans l'ILA était l'idée selon laquelle, si un contractant est chargé, par un responsable du traitement, de traiter des données à des fins vaguement définies, cela crée un risque que le contractant définisse lui-même, dans une plus ou moins large mesure, ces finalités.

Un pouvoir discrétionnaire implicite, de portée ambiguë et avec des finalités vaguement définies, confère effectivement à un sous-traitant une autorisation d'agir en tant que responsable du traitement d'une manière qui peut rester entièrement cachée à une organisation qui fait l'acquisition de ses services.

Dans un contrat impliquant un traitement à grande échelle ou autrement à haut risque, cela expose de manière significative les personnes concernées. Il pourrait en résulter qu'une grande quantité de données à caractère personnel soient traitées selon les manières déterminées par le contractant,

plutôt que selon les instructions de l'organisation acquéreuse. Dans la mesure où le contractant agit en qualité de responsable du traitement, la capacité de l'organisation acquéreuse à lui demander des comptes sur ses activités de traitement sera très limitée.

Si une organisation publique achète les services d'un contractant et lui accorde le pouvoir discrétionnaire d'agir en tant que responsable du traitement en vertu du RGPD, elle génère un risque supplémentaire qui est spécifique au mandat d'intérêt général de cette organisation. En vertu du RGPD, le traitement peut être effectué de manière licite dans le respect des intérêts légitimes du responsable du traitement. Comme expliqué, l'addendum sur la protection des données permet à Microsoft d'effectuer le traitement en tant que responsable du traitement, ce qui semblerait rentrer dans ce cadre. Toutefois, le RGPD ne permet pas que le traitement fondé sur l'intérêt légitime d'un responsable du traitement soit réalisé par les autorités publiques dans l'exercice de leurs fonctions. Un traitement par les institutions de l'UE au titre du règlement (UE) 2018/1725 ne présente pas non plus d'intérêt légitime. **Le considérant 25 et l'article 6 du règlement (UE) 2018/1725** [*voir également le considérant 50 et l'article 6, paragraphe 4, du RGPD*] indiquent que lorsque les institutions de l'UE utilisent des produits et services informatiques pour exécuter des tâches d'intérêt général qui leur sont confiées par le droit de l'UE, tout traitement destiné à des tâches et des finalités autres devrait être compatible avec les missions et les rôles des institutions de l'UE. Lorsque les institutions de l'UE agissent en qualité de responsables du traitement, elles doivent vérifier si les finalités pour lesquelles d'autres traitements ou un traitement ultérieur sont effectués sont compatibles au titre de l'**article 6 du règlement (UE) 2018/1725** [*voir également l'article 6, paragraphe 4, du RGPD*].

Les pouvoirs publics peuvent désirer examiner si, à la lumière des tâches qu'ils accomplissent dans l'intérêt public, ils jugent opportun qu'un contractant devienne un responsable du traitement - ou même un responsable conjoint du traitement - des données à caractère personnel des agents du personnel et des citoyens du seul fait de la nécessité, pour l'autorité concernée, d'externaliser ses tâches informatiques. Dans son enquête, le CEPD a constaté l'existence d'un risque que les protections conçues pour le contexte d'intérêt général, dans lequel des données à

caractère personnel ont été confiées aux institutions de l'UE, soient contournées par le biais du processus d'externalisation.

## 2.5 Recommandations

Du point de vue du CEPD, les risques présentés par la situation dans laquelle Microsoft avait la responsabilité du traitement l'emportaient sur les avantages qu'un tel dispositif pouvait offrir aux institutions de l'UE. La ligne d'action que le CEPD a recommandée aux institutions de l'UE comportait ce qui suit.

- Chaque institution de l'UE devrait être seule responsable du traitement pour son utilisation des produits et services de Microsoft lorsqu'elle accomplit des tâches d'intérêt général ou relevant de l'exercice de l'autorité publique.
- L'accord-cadre devrait prévoir une hiérarchie claire des documents contractuels.
- Les modifications négociées apportées par les institutions de l'UE aux conditions générales de Microsoft devraient figurer dans le document contractuel de plus haut rang. Il en va de même pour toutes les dispositions nécessaires pour la conformité au règlement (UE) 2018/1725.
- Ce n'est que d'un commun accord qu'il devrait être possible de modifier les dispositions de l'ILA intéressant la protection des données.
- La portée des dispositions de l'ILA qui concernent la protection des données devrait être étendue à toutes les données à caractère personnel non seulement fournies à Microsoft mais également générées par Microsoft, du fait de l'utilisation par les institutions de l'UE de tous les produits et services de Microsoft.
- Les institutions de l'UE devraient négocier un ensemble précis, explicite et exhaustif de finalités pour couvrir tous les types de données à caractère personnel liés à leur utilisation de produits et services de Microsoft. Il convient de limiter les finalités à celles qui sont nécessaires pour que les institutions de l'UE utilisent ces produits et services. Il y a lieu d'interdire expressément d'autres finalités.

# 3 Accord entre le responsable du traitement et le sous-traitant

## 3.1 Exhaustivité de l'accord

### 3.1.1 Évaluation

Selon le CEPD, si les institutions de l'UE devaient demeurer les seules responsables du traitement des données à caractère personnel traitées au titre de l'ILA, leur accord responsable du traitement/sous-traitant signé avec Microsoft devait être considérablement renforcé. Bon nombre des éléments nécessaires soit ont été mal mis en œuvre, soit sont absents.

Les exigences relatives à un accord responsable du traitement/sous-traitant conforme sont énoncées à l'**article 29 du règlement (UE) 2018/1725** [*voir également l'article 28 du RGPD*]. Elles sont omniprésentes dans le présent document. L'article 29, paragraphe 3, du règlement (UE) 2018/1725 exige que l'accord entre le responsable du traitement et le sous-traitant «lie le sous-traitant à l'égard du responsable du traitement»[22]. Il n'y a donc pas lieu qu'un sous-traitant dispose d'un droit illimité de modification unilatérale aux termes d'un accord entre le responsable du traitement et lui-même. Un sous-traitant ne devrait procéder au traitement que sur la base d'instructions documentées fournies par le responsable du traitement.

L'article 29, paragraphe 3, du règlement (UE) 2018/1725 exige que l'accord entre le responsable du traitement et le sous-traitant indique «le type de données à caractère personnel et les catégories de personnes concernées, ainsi que les obligations et les droits du responsable du traitement.»[23] L'analyse du CEPD avait conclu qu'il était difficile de savoir quels contrôles contractuels, s'il en existait, s'appliquaient aux différentes catégories de données traitées par Microsoft dans le cadre de l'ILA. Comme l'a montré le CEPD, bien que Microsoft ait eu des obligations et des droits caractéristiques d'un responsable du traitement en vertu de l'ILA, ces derniers n'étaient généralement pas expressément mentionnés. Par suite, les obligations et les droits des institutions de l'UE en tant que responsables du traitement n'étaient pas entièrement définis. Les documents négociés de l'ILA ne faisaient nulle mention des catégories de personnes concernées, bien que

ces dernières aient été mentionnées dans l'addendum sur la protection des données.

L'article 29, paragraphe 3, du règlement (UE) 2018/1725 exige également que l'accord entre le responsable du traitement et le sous-traitant définisse «l'objet [...], la nature et la finalité du traitement»[24]. L'analyse par le CEPD de la limitation des finalités contractuelles a montré que cela a été fait avec une précision insuffisante.

Dans cette section, le CEPD s'intéresse surtout à deux autres points essentiels de non-respect de l'article 29 du règlement (UE) 2018/1725: premièrement, le défaut de contrôle accordé aux institutions de l'UE sur l'utilisation de sous-traitants ultérieurs par Microsoft et, deuxièmement, l'absence de droits d'audit efficaces accordés à ces mêmes institutions.

### 3.1.2 Recommandations

Le CEPD a recommandé que les institutions de l'UE prennent les mesures suivantes.

- Établir un accord global entre responsable du traitement et sous-traitant qui comporte les rôles et les responsabilités du sous-traitant et du responsable du traitement, l'objet, la durée et la nature du traitement, les types de données à caractère personnel concernés, les catégories de personnes concernées, les obligations et les droits des responsables du traitement et des sous-traitants.
- Les types de données à caractère personnel et les catégories de personnes concernées devraient être précisés aussi exactement que possible afin de garantir le respect des principes de base, tels que la minimisation des données, les limitations des finalités et la licéité du traitement.
- Les instructions documentées fournies par les institutions de l'UE au titre de l'ILA devraient couvrir, par exemple, les types de données pouvant être traitées, les personnes pouvant avoir accès aux données, la manière et l'endroit où celles-ci sont stockées, les mesures de sécurité mises en place, la question de savoir si les transferts vers des pays tiers sont autorisés et, dans l'affirmative, vers quels destinataires, vers quels pays et dans quelles conditions. Les instructions doivent être

incluses dans le contrat et, en ce qui concerne les autres instructions, il importe de s'accorder sur les modèles et procédures nécessaires et de les annexer au contrat.

## 3.2 Sous-traitants ultérieurs

### 3.2.1 Évaluation

Les responsables du traitement sont tenus de permettre que le traitement soit effectué pour leur compte uniquement par des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures pour la protection des droits des personnes concernées[25]. En tant que sous-traitant, la société Microsoft n'est pas autorisée à recruter un autre sous-traitant sans l'autorisation écrite préalable du responsable du traitement[26]. Si elle engage un autre sous-traitant alors qu'elle ne dispose que d'une autorisation écrite générale, elle doit donner au responsable du traitement une possibilité réelle d'approuver une liste de sous-traitants au moment de la signature de l'autorisation générale et une possibilité réelle d'émettre des objections à l'encontre de toute modification ultérieure portant sur les sous-traitants qu'elle engage[27].

En tant que sous-traitant, Microsoft doit également transmettre par contrat à ses sous-traitants les mêmes obligations en matière de protection des données dans le cadre de l'accord de licence[28]. Parmi les obligations devant être transmises se trouvent les engagements pris par Microsoft quant à la mise en œuvre des mesures techniques et organisationnelles que le responsable du traitement estime nécessaires[29]. Eu égard aux obligations de rendre compte incombant aux responsables du traitement[30], ceux-ci devraient être en mesure de démontrer que Microsoft s'est conformée à ses engagements.

L'intention qui sous-tend les dispositions du règlement (UE) 2018/1725 (et du RGPD) concernant les sous-traitants ultérieurs consiste à mettre les responsables du traitement en mesure d'exercer leur contrôle, de sorte qu'ils puissent s'acquitter de leurs obligations de protection des droits des personnes concernées. Selon le CEPD, l'ILA ne permettait pas aux institutions de l'UE d'exercer un contrôle sur les sous-traitants ultérieurs engagés par Microsoft. Il présentait donc un risque pour les personnes concernées.

L'absence de contrôle de la part des institutions de l'Union était manifeste au regard des trois éléments suivants.

Premièrement, les conditions négociées en matière de protection des données figurant dans l'accord-cadre contenaient ce qui semblait être une autorisation générale d'engager des sous-traitants ultérieurs. Toutefois, à l'instar de nombreuses obligations en matière de protection des données au titre de l'ILA, elle ne s'appliquait qu'aux données à caractère personnel *fournies* par l'utilisation des *services en ligne*. Le CEPD n'a constaté aucune autorisation en place pour les autres catégories de données traitées par Microsoft, en vertu de l'ILA.

Deuxièmement, selon le CEPD, dans la pratique, les informations fournies aux institutions de l'UE sur les nouveaux sous-traitants ultérieurs comprenaient le nom du sous-traitant ultérieur, le type général de service qu'il fournissait et le pays de son siège social[31]. Le CEPD n'a pas jugé ces informations suffisantes. De l'avis du CEPD, pour qu'un système d'autorisation générale offre aux institutions de l'UE une possibilité réelle d'exprimer des objections à l'encontre de nouveaux sous-traitants ultérieurs, ces institutions devraient également savoir quels types de traitements les sous-traitants potentiels devaient se voir confier, en rapport avec quels produits et services spécifiques, avec quelles garanties pour la protection des données et quelles mesures de sécurité en place. Sans ces informations, les institutions de l'UE ne pouvaient pas démontrer pourquoi elles avaient raison d'agréer les sous-traitants en question et ne pouvaient donc être tenues de rendre compte de leur décision.

Troisièmement, si les institutions de l'UE n'approuvaient pas un nouveau sous-traitant ultérieur, leur seul recours dans les conditions négociées de l'ILA était de mettre fin à leur abonnement au service en ligne concerné. Si le service en ligne concerné faisait partie d'une suite, le seul recours des institutions de l'UE était la résiliation de leur abonnement pour l'ensemble de la suite.

Cette solution contractuelle risquait d'être sans effet dans la pratique. Le CEPD estime qu'il existait un risque que les institutions de l'UE se trouvent sans alternative réaliste à l'utilisation du service ou de la suite Microsoft concernés si elles exprimaient des objections concernant un nouveau sous-

traitant ultérieur. Dans de telles circonstances, elles n'auraient effectivement pas le moindre mot à dire sur le choix du sous-traitant ultérieur.

Selon le CEPD, il était essentiel que les institutions de l'UE soient en mesure de refuser un sous-traitant ultérieur si elles avaient des raisons de penser qu'il présentait un risque sur le plan de la conformité. Tel pourrait être le cas si, par exemple, les audits révélaient des problèmes de conformité chez ce sous-traitant.

En effet, il est probable que tout responsable qui sous-traite de vastes opérations de traitement ou un autre type de traitement à haut risque devra être en mesure de donner un agrément significatif aux sous-traitants ultérieurs qui seront utilisés par le contractant s'il veut respecter ses propres obligations de conformité.

### 3.2.2 Recommandations

Le CEPD a recommandé que les institutions de l'UE prennent les mesures suivantes.

- Évaluer les risques pour les personnes concernées générés par les sous-traitants ultérieurs actuellement utilisés par Microsoft.
- Veiller à ce que le recours à des sous-traitants ultérieurs pour toutes les données à caractère personnel traitées par Microsoft en vertu de l'ILA (et tout changement de sous-traitant ultérieur) soit soumis à une autorisation écrite préalable.
- Introduire dans l'ILA l'obligation pour Microsoft de fournir des informations complètes, premièrement, sur les sous-traitants ultérieurs qui ont été utilisés pour chaque produit ou service fourni aux institutions de l'UE et pour chaque activité de traitement et chaque catégorie de données à caractère personnel; et deuxièmement, sur les mesures de sécurité et les mesures visant à la protection des données (à savoir, des mesures techniques et organisationnelles) mises en place concernant chaque sous-traitant ultérieur. Cela devrait inclure l'obligation, pour Microsoft, de fournir, sur demande, les parties pertinentes de son contrat avec un sous-traitant ultérieur donné.

- Introduire des garanties dans l'ILA pour faire en sorte que l'autorisation préalable soit accordée librement en ce qui concerne chaque sous-traitant engagé par Microsoft. Les institutions de l'UE devraient être en mesure de refuser un sous-traitant ultérieur particulier sans subir de baisse de service de ce fait.

## 3.3 Droits d'audit

### 3.3.1 Évaluation

Conformément à l'**article 29, paragraphe 3, point h), du règlement (UE) 2018/1725** [*voir également l'article 28, paragraphe 3, point h), du RGPD*], un accord entre le responsable du traitement et le sous-traitant doit contenir deux obligations à la charge du sous-traitant. Premièrement, le sous-traitant doit mettre à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de l'ensemble de l'article 29 du règlement (UE) 2018/1725. Deuxièmement, le sous-traitant doit se soumettre aux audits et aux inspections du responsable du traitement. Ces obligations sont cumulatives: en conséquence, le sous-traitant doit accéder à toute demande raisonnable relevant de l'une ou l'autre de ces obligations. Elles doivent également être imposées par contrat aux sous-traitants ultérieurs[32].

Compte tenu de l'obligation de rendre compte incombant au responsable du traitement en vertu de l'**article 26 du règlement (UE) 2018/1725** [*voir également l'article 24 du RGPD*], le détail et la portée des droits d'audit prévus dans le contrat devraient refléter «la nature, la portée, le contexte et les finalités du traitement ainsi que les risques [...] pour les droits et libertés des personnes physiques». Compte tenu de la grande quantité de données traitées du fait de l'utilisation des produits et des services Microsoft par les institutions de l'UE, du grand nombre de personnes concernées et du manque de clarté concernant ce qui, exactement, a été traité, où, comment et à quelles fins, les circonstances dans lesquelles le CEPD a mené son enquête commandaient aux institutions de l'UE de mettre en œuvre des dispositions d'audit solides et efficaces. Ces dispositions devaient être un ensemble d'instructions claires, contraignantes et détaillées fournies à Microsoft par les institutions de l'UE concernant la réalisation des audits.

En vertu de l'article 29, paragraphe 3, deuxième alinéa, du règlement (UE) 2018/1725, une obligation supplémentaire imposée au sous-traitant est d'informer immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du règlement ou de la législation de l'UE ou des État membres en matière de protection des données[33]. Eu égard aux obligations de conformité du sous-traitant, il s'agit là d'une obligation qui lui est faite d'informer le responsable du traitement de manière proactive s'il détecte un problème de conformité avec les instructions qu'il reçoit de celui-ci.

Les conditions négociées figurant dans l'ILA reproduisaient le libellé des obligations statutaires au titre de l'article 29, paragraphe 3, du règlement (UE) 2018/1725, qui viennent d'être citées[34]. Elles ne fournissaient aucun détail sur ce que les institutions de l'UE pouvaient attendre de Microsoft pour les respecter.

Quelques précisions supplémentaires ont été fournies dans l'addendum sur la protection des données. Le CEPD a appris que Microsoft veillerait à ce que les *audits de sécurité* soient réalisés au moins une fois par an par des *auditeurs de sécurité* externes sélectionnés et payés par Microsoft.

Les textes n'expliquaient pas dans quelle mesure ces audits de sécurité porteraient sur le respect de la protection des données. Cette omission était significative: il est possible d'obtenir d'excellents résultats à un audit de sécurité tout en échouant à un audit sur la protection des données en raison d'un manque de transparence, d'un traitement ultérieur illicite ou d'autres problèmes relatifs à la protection des données.

Les textes ne confirmaient pas non plus si les audits de sécurité couvriraient toutes les activités de traitement relevant du champ d'application des conditions relatives aux services en ligne ou seulement certaines, ou couvriraient également le traitement en dehors du champ d'application des conditions relatives aux services en ligne. Ils n'expliquaient pas si les sous-traitants ultérieurs étaient couverts. Les données sur les services professionnels semblaient exclues du champ d'application des audits de sécurité[35], conjointement avec un certain nombre de services en ligne[36].

Lues dans leur ensemble, les dispositions en matière d'audit figurant dans l'addendum sur la protection des données ont également suggéré que les

audits de sécurité propres à Microsoft constituaient le point de départ pour parvenir à un «respect des audits»[37].

Le CEPD estime qu'il s'agit là d'une hypothèse erronée. Les audits relatifs à la protection des données, qui évaluent le respect des obligations imposées par le règlement (UE) 2018/1725, ont un champ d'application plus large et appliquent des normes différentes de celles des audits de sécurité. En outre, les audits commandés par la société Microsoft *elle-même* avec une portée (limitée) de *son* choix ne pourraient jamais équivaloir aux droits d'audit réels des responsables du traitement prévus par le règlement (UE) 2018/1725. En effet, l'article 29, paragraphe 3, point h), du règlement (UE) 2018/1725 impose à Microsoft une obligation contractuelle d'autoriser les audits «[réalisés] par le responsable du traitement» ou «[un autre auditeur] qu'il a mandaté»[38].

L'addendum sur la protection des données contenait un engagement de Microsoft à «répondre rapidement» aux instructions d'audit supplémentaires, «[d]ans la mesure où les exigences d'audit du client [...] ne peuvent raisonnablement pas être satisfaites par les rapports d'audit, la documentation ou les informations de conformité que Microsoft met généralement à la disposition de ses clients»[39].

Le CEPD a décelé deux problèmes en lien avec ce libellé. Premièrement, les informations fournies par Microsoft et les auditeurs mandatés par Microsoft pourraient fournir aux institutions de l'UE un certain niveau d'assurance. Mais elles ne sauraient se substituer à la capacité des institutions de l'UE à recueillir et à vérifier les preuves relatives aux déclarations mêmes de Microsoft. Les informations fournies par Microsoft et par ses auditeurs n'étaient donc pas un moyen par lequel les exigences en matière d'audit propres aux institutions de l'UE pouvaient être «raisonnablement satisfaites». Elles étaient plutôt un moyen par lequel les institutions de l'UE pouvaient déterminer les domaines sur lesquels concentrer leurs contrôles.

Deuxièmement, il ne suffisait pas que Microsoft «réponde» rapidement aux instructions données par les institutions de l'UE concernant les audits. Refuser à ces institutions de réaliser un audit dont le champ d'application recoupe celui de ses propres audits pouvait constituer une réponse. Ce pouvoir discrétionnaire appartient comme il se doit à un responsable du traitement.

Dans l'ensemble, les droits d'audit des institutions de l'UE au titre de l'ILA n'étaient pas suffisamment solides compte tenu des risques présentés par le traitement. Il existait également un manque de précision manifeste quant à la manière dont Microsoft devait remplir son obligation de permettre et de contribuer aux audits. Enfin, le champ d'application de ces droits était trop étroit. Les institutions de l'UE risquaient d'être incapables de demander des comptes à Microsoft et, par conséquent, incapables de s'acquitter de leur propre obligation de rendre des comptes.

Le CEPD comprend qu'un fournisseur de services à très grande échelle souhaiterait éviter de se retrouver avec un nombre impossible à maîtriser d'audits différents réalisés par des clients différents. Toutefois, le règlement (UE) 2018/1725 est clair: les responsables du traitement doivent être en mesure d'auditer les sous-traitants et les sous-traitants ultérieurs. Le CEPD a également estimé qu'il devrait être possible d'organiser des audits qui satisfassent plusieurs clients en même temps.

### 3.3.2 Recommandations

Le CEPD a formulé les recommandations ci-après aux institutions de l'UE.

- Il convient de modifier l'ILA afin de donner au responsable du traitement et au CEPD des droits d'audit détaillés, efficaces et applicables.
- L'ILA devrait également exiger de la société Microsoft qu'elle mette à la disposition des institutions de l'UE toutes les informations nécessaires pour démontrer son respect de l'article 29 du règlement (UE) 2018/1725. Les dispositions contractuelles devraient, de l'avis du CEPD, couvrir les informations concernant le fonctionnement des systèmes utilisés, l'accès aux données et aux destinataires, les sous-traitants ultérieurs, les mesures de sécurité, la conservation des données à caractère personnel, la localisation des données, les transferts de données à caractère personnel ou tout autre traitement ultérieur des données à caractère personnel. Lorsque Microsoft apporte des modifications substantielles qui sont pertinentes du point de vue de la protection des données, elle devrait également être tenue de notifier les institutions de l'UE de manière à

les inciter à consulter et à évaluer les informations relatives à ces modifications.

- L'ILA devrait comprendre des dispositions précisant la manière dont Microsoft doit appliquer en pratique les obligations qui lui incombent en vertu de l'article 29, paragraphe 3, deuxième alinéa, du règlement (UE) 2018/1725.
- En tant que responsables du traitement, les institutions de l'UE devraient mettre en place un programme d'audit consistant en des contrôles réguliers réalisés par leur équipe d'audit interne ou externe. La portée et la fréquence des audits devraient refléter l'ampleur du traitement et les risques pour les personnes concernées.
- Les audits réalisés dans le cadre de l'ILA devraient recueillir des preuves factuelles du respect par Microsoft des obligations qui lui incombent.
- Les résultats d'audit significatifs devraient être communiqués aux niveaux appropriés de la hiérarchie au sein des institutions de l'UE. Les résultats devraient permettre à celles-ci de mettre en évidence et de donner suite aux éventuels problèmes de conformité. Ils devraient également être fournis au CEPD à sa demande.

# 4 Localisation, transferts et divulgation des données

L'enquête du CEPD a montré que les institutions de l'UE n'étaient pas en mesure de contrôler la localisation d'une grande partie des données traitées par Microsoft. Elles n'avaient pas non plus un contrôle total sur les données qui étaient transférées hors de l'UE/EEE et sur la manière dont le transfert était effectué. Les garanties adéquates faisaient aussi défaut pour la protection des données quittant l'UE/EEE. Cette situation a eu une incidence négative concrète sur la capacité des institutions de l'UE à demander des comptes à Microsoft.

Les institutions de l'UE avaient également peu de garanties qu'elles étaient en mesure de défendre les privilèges et immunités qui leur étaient accordés en vertu du traité sur le fonctionnement de l'Union européenne («TFUE») et que Microsoft ne divulguerait des données à caractère personnel que dans la mesure où le droit de l'Union l'y autorisait.

Dans cette section, le CEPD examine tour à tour les problèmes qui se recoupent concernant la localisation des données, les transferts internationaux et la communication des informations.

## 4.1 Localisation des données

Au moment où le CEPD a clôturé son enquête en mars 2020, l'emplacement (de stockage) de (certaines) données était précisé dans les conditions relatives aux Services en ligne[40]. Aux termes desdites conditions, l'obligation de stocker les données dans l'UE ne s'appliquait qu'à un *sous-ensemble* des données *fournies* par l'utilisation de certains «*services en ligne Core*».

Ces *services en ligne Core* incluaient les services Microsoft Office 365 et certains services *Microsoft Azure*.[41] Microsoft s'est engagée à conserver dans l'UE une partie seulement des données fournies par l'utilisation de ces services. Pour les services de l'Office 365, Microsoft s'est engagée à stocker dans l'UE uniquement le contenu de la boîte aux lettres *Exchange Online*, le contenu du site *SharePoint Online* et les fichiers téléchargés vers *OneDrive for Business*. Les données fournies par l'utilisation d'autres services de l'Office 365 n'étaient pas concernées, pas plus que les informations sur l'identité des utilisateurs ou les métadonnées. Pour les services de base *Microsoft Azure*, comme *Azure Active Directory* (utilisé pour la gestion de l'identité des utilisateurs dans les services en ligne de Microsoft), les conditions relatives aux services en ligne prévoyaient expressément que: «certains services sont susceptibles de ne pas permettre au client de configurer le déploiement dans [l'UE/l'EEE] ou en dehors des États-Unis et stocker des copies de sauvegarde à d'autres emplacements.»[42]

L'addendum sur la protection des données précisait également que «[s]auf dans les conditions prévues dans les Conditions du DPA, les données client et les données à caractère personnel que Microsoft traite pour le compte du client peuvent être transférées, stockées et traitées aux États-Unis ou dans tout autre pays dans lequel Microsoft ou ses sous-traitants ultérieurs opèrent»[43].

L'obligation de stocker des données dans l'UE/EEE ne s'appliquait donc qu'à un sous-ensemble des données traitées par Microsoft lorsqu'elle fournissait des «services en ligne Core». L'emplacement de stockage des données ne

relevant pas de ce sous-ensemble n'était pas clairement indiqué, tout comme l'emplacement des données qui étaient transférées hors de l'UE/EEE.

Les conditions négociées dans l'accord-cadre permettaient que les données *recueillies* par la société Microsoft soient situées en tout lieu choisi par elle.

Dans la mesure où la société collectait, en tant que responsable du traitement, des données à caractère personnel à partir de produits et services, la déclaration de confidentialité de Microsoft n'était pas contraignante[44].

Les institutions de l'UE n'étaient donc pas libres de décider de l'endroit où stocker leurs données. Elles n'étaient pas non plus libres de décider de procéder à des transferts hors de l'UE/EEE. Selon le CEPD, les dispositions prévues dans l'ILA et la déclaration de confidentialité de Microsoft ne permettaient même pas aux institutions de l'UE de déterminer l'emplacement de tous les différents types de données à caractère personnel traitées en vertu de ces dispositions.

## 4.2 Transferts internationaux

Lorsque des transferts internationaux vers des pays tiers ou à des organisations internationales sont nécessaires, ils ne devraient être effectués que dans le strict respect des règles applicables en matière de transfert[45] et à la suite d'une évaluation documentée des risques qu'ils présentent pour les droits et libertés des personnes concernées. Il incombe aux responsables du traitement de décider s'ils autorisent ou non un transfert.

Selon le CEPD, les institutions de l'UE avaient signé l'ILA avec Microsoft Irlande. Toujours selon le CEPD, dans le cadre de l'ILA, les garanties qui avaient été mises en place conformément aux règles internationales en matière de transfert avaient jusqu'à présent été contractuelles. À la connaissance du CEPD, le groupe Microsoft n'avait pas adopté de règles d'entreprise contraignantes en vigueur qui soient autorisées en vertu du RGPD ou des instruments précédents.

En vertu de l'addendum sur la protection des données, en signant l'ILA, les institutions de l'UE sont réputées avoir également signé un ensemble de clauses contractuelles types («CCT») pour les transferts internationaux de

données, avec Microsoft Corporation[46]. En conséquence, les institutions de l'UE avaient à la fois une relation directe avec un sous-traitant établi dans l'UE (Microsoft Irlande) qui pouvait effectuer des transferts internationaux à ses sous-traitants et une relation directe avec Microsoft Corporation en tant que sous-traitant établi hors de l'UE/EEE qui pouvait également effectuer des transferts internationaux vers ses sous-traitants ultérieurs. Selon le CEPD, la grande majorité du traitement des données à caractère personnel était en pratique effectué par Microsoft Corporation et ses sous-traitants ultérieurs, et non par Microsoft Irlande et ses sous-traitants ultérieurs.

Compte tenu de cette matrice contractuelle, les institutions de l'UE avaient besoin des deux niveaux de garanties contractuelles suivants. Premièrement, il fallait qu'elles donnent, dans l'ILA, des instructions à Microsoft Irlande et à Microsoft Corporation sur le point de savoir dans quelle mesure, dans quelles conditions et sous réserve de quelles garanties des données à caractère personnel pouvaient être transférées hors de l'UE/EEE. Ces conditions et ces garanties devaient se retrouver dans les clauses contractuelles types concernant les transferts signées par les institutions de l'UE avec Microsoft Corporation. Compte tenu de ce scénario, il serait approprié d'utiliser les CCT adoptées en vertu de l'article 48, paragraphe 2, point b) ou c), du règlement (UE) 2018/1725[47] entre les institutions de l'UE et Microsoft Corporation. Toutefois, étant donné qu'il n'existe pas encore de CCT de ce genre, les institutions de l'UE pourraient, à titre de mesure provisoire, utiliser les dispositions des CCT telles que celles adoptées en vertu de la décision 2010/87/UE de la Commission, sous réserve de l'autorisation du CEPD en vertu de l'article 48, paragraphe 3, point a), du règlement (UE) 2018/1725.

La position dans le cadre de l'ILA était différente, dans la mesure où, selon le CEPD, les problèmes suivants se posaient.

Premièrement, comme expliqué dans la sous-section précédente relative à la localisation des données, les instructions figurant dans l'ILA sur les données à caractère personnel que Microsoft pouvait transférer hors de l'UE/EEE, à quel moment et avec quelles finalités, étaient limitées en termes de champ d'application et insuffisantes.

Deuxièmement, les instructions des institutions européennes sur les garanties qui devaient régir ces transferts manquaient de précision. L'accord-

cadre négocié engageait, pour l'essentiel, Microsoft à respecter ses obligations statutaires et ne donnait aucune précision quant à la manière dont il convenait de les mettre en œuvre.

Troisièmement, il n'était pas certain que les instructions des institutions de l'UE figurant dans les documents négociés de l'ILA étaient censées lier Microsoft Corporation de même que Microsoft Irlande. Microsoft Corporation n'était pas expressément liée et, à la connaissance du CEPD, n'était pas signataire de ces documents. Compte tenu de la matrice contractuelle, le CEPD a estimé qu'il était nécessaire que les instructions des institutions de l'UE soient, sans ambiguïté aucune, contraignantes pour les deux entités.

Quatrièmement, les CCT concernant les transferts, que Microsoft Corporation a contresignées, n'étaient pas conformes. Les préoccupations du CEPD étaient les suivantes.

**Les responsables du traitement souhaitant utiliser les CCT concernant les transferts adoptées par la Commission européenne (telles que les clauses types adoptées au titre de la décision 2010/87/UE de la Commission) doivent compléter les annexes** afin de préciser l'objet, la durée, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, ainsi que les mesures de sécurité à appliquer aux données transférées[48]. Le contenu des annexes devrait être adapté à chaque **produit et service concerné et à chaque destinataire (y compris les sous-traitants ultérieurs)**. Alors seulement la description faite peut correspondre à la relation spécifique entre responsable du traitement et sous-traitant concernée.

Dans sa mise en œuvre standard de ces CCT pour les transferts, Microsoft a prérempli la description du traitement dans les annexes[49]. Les listes des personnes concernées et des catégories de données étaient génériques et rédigées dans les grandes lignes, dans la mesure où elles étaient conçues pour être les mêmes pour n'importe quel client. En fonction des besoins opérationnels de chaque institution de l'UE, il se peut que certaines catégories ne soient pas valables ou que d'autres relèvent du fourre-tout constitué par la formule «[t]oute autre donnée à caractère personnel». La formulation des annexes visait à surmonter le caractère générique des listes en indiquant que «[l]e client peut choisir d'inclure, dans les données à

caractère personnel, des données de l'une des catégories suivantes [types de personnes concernées/catégories de données] dans les données clients». Or, cela allait à l'encontre de l'objectif visant à décrire clairement la portée du transfert.

Étant donné que les CCT pour les transferts devaient être spécifiques à chaque relation entre responsable du traitement et sous-traitant, il n'était pas non plus approprié qu'elles soient négociées (ou imposées par Microsoft) au moment de leur intégration dans un accord-cadre intéressant un grand nombre d'institutions de l'UE.

Chaque responsable du traitement devrait être en mesure de préciser le traitement considéré dans les CCT pour les transferts qu'il conclut avec Microsoft Corporation. Une option de mise en conformité consisterait en un ensemble de clauses comprenant un système de cases à cocher dans les annexes, que les différents responsables du traitement devraient compléter et contresigner.

Comme pour beaucoup d'autres engagements prévus dans l'ILA, ces CCT pour les transferts ne s'appliquent qu'aux données fournies par l'utilisation de services en ligne. Le CEPD n'avait pas connaissance de l'existence d'un mécanisme contractuel correspondant pour les produits et services qui n'étaient pas des services en ligne, ou pour les données collectées et traitées par Microsoft en tant que responsable du traitement. De l'avis du CEPD, si ces données devaient être simplement traitées ou transférées, elles devaient être réglementées dans le cadre de l'ILA. Les instructions des institutions de l'UE à ce niveau devaient ensuite figurer dans les CCT pour les transferts signées avec Microsoft Corporation et dans toute nouvelle CCT que Microsoft Corporation concluait avec des sous-traitants ultérieurs au sujet de transferts qui leur étaient destinés.

Enfin, étant donné que les CCT n'étaient conformes que si les parties n'avaient apporté aucun changement à ces conditions (autre que le fait de remplir les annexes), elles devaient prévaloir sur d'autres conditions contractuelles dans la hiérarchie des documents contractuels de l'ILA. Ce point n'était pas certain, compte tenu du caractère ambigu de la hiérarchie établie dans d'autres documents contractuels composant l'ILA.

## 4.3 Divulgation non autorisée

Le protocole nº 7 du traité sur le fonctionnement de l'Union européenne prévoit l'inviolabilité des biens, des avoirs, des archives, des communications et des documents de l'UE. Il ressort du protocole nº 7 qu'un sous-traitant engagé par des institutions de l'UE doit uniquement divulguer des données à caractère personnel qu'il traite pour le compte des institutions de l'UE s'il en informe l'institution de l'UE concernée et obtient son accord, ou s'il a l'autorisation de la Cour de justice[50]. Les institutions de l'Union ne perdent pas le bénéfice de la protection offerte par le protocole simplement parce qu'elles dépendent d'un prestataire externe pour certains services.

**L'article 49 du règlement (UE) 2018/1725** [*voir également l'article 48 du RGPD*] dispose que toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant la divulgation de données à caractère personnel ne peut être [...] rendue exécutoire [...] qu'à la condition qu'elle soit fondée sur un accord international auquel l'UE est partie[51].

L'article 4, paragraphe 1, point f), du règlement (UE) 2018/1725 impose aux institutions de l'UE de garantir l'intégrité et la confidentialité des données à caractère personnel traitées pour leur compte[52].

Ces obligations juridiques s'accompagnaient difficilement des dispositions de l'ILA sur la divulgation. L'addendum sur la protection des données permettait à Microsoft de répondre positivement aux demandes d'accès aux données lorsqu'elle estimait qu'elle était juridiquement tenue de le faire[53]. Microsoft n'aurait même pas informé les clients d'une demande en cas d'«interdiction légale».[54]. Bien sûr, l'addendum sur la protection des données ne couvrait qu'un sous-ensemble de données à caractère personnel traitées au titre de l'ILA. À la connaissance du CEPD, aucun engagement contractuel n'a été pris concernant des divulgations portant sur des données à caractère personnel ne relevant pas de ce sous-ensemble.

Compte tenu de l'analyse effectuée par le CEPD, selon laquelle Microsoft a conservé un pouvoir discrétionnaire pour traiter des données en tant que responsable du traitement, une partie au moins de ces données risquait d'être régie par les politiques de Microsoft mentionnées dans sa déclaration de confidentialité. Cela a permis à Microsoft de divulguer des données à caractère personnel (y compris les données clients, les données administrateurs, les données de paiement et les données de support) à des tiers, notamment aux services répressifs ou à d'autres organismes publics[55].

Le protocole nº 7 et le règlement (UE) 2018/1725 protègent les institutions de l'Union des demandes de divulgation que des sous-traitants qu'elles ont engagés pourraient recevoir des gouvernements des États membres de l'UE. Il est possible que le protocole et le règlement ne puissent pas protéger les institutions de l'UE contre les demandes de divulgation émanant de gouvernements de pays tiers et de sous-traitants relevant de leur compétence. En fonction des lois de ce pays tiers et de leur portée extraterritoriale, ces sous-traitants peuvent être confrontés à un conflit de lois et juger prudent de se conformer aux lois du pays tiers, même si cela les met en position d'enfreindre les lois de l'Union.

Par conséquent, si les institutions de l'UE font appel à des sous-traitants ayant des liens avec les gouvernements de pays tiers, elles peuvent, dans la pratique, en venir à faire le choix de renoncer aux protections offertes par le protocole et le règlement contre la divulgation non autorisée.

## 4.4 Conséquences

Compte tenu de la situation prévalant en vertu de l'ILA et des circonstances de la relation entre les institutions de l'UE et Microsoft, les difficultés pratiques suivantes se sont posées.

Si les données à caractère personnel des utilisateurs des institutions de l'UE et d'autres personnes concernées étaient localisées et traitées en dehors de l'UE/EEE, il devenait beaucoup plus difficile pour les institutions de l'UE de mettre en place des mesures efficaces pour garantir le respect du règlement (UE) 2018/1725 et vérifier leur respect des dispositions en tant que responsables du traitement.

Un manque d'information et de contrôle sur les données en transit était également préoccupant. Les flux transfrontières de données à caractère personnel s'accompagnent d'un risque de rupture dans la continuité du niveau de protection assuré au sein de l'UE[56]. Sans une image précise des pays par lesquels les données sont susceptibles de transiter, il devient très difficile pour les institutions de l'UE d'évaluer quelles garanties techniques, organisationnelles, sécuritaires et contractuelles elles doivent mettre en œuvre avant l'ouverture d'un transfert. Par conséquent, elles risquent de compromettre leur mise en œuvre des principes régissant la protection des données (par exemple, la minimisation des données, la limitation des

finalités) ainsi que la confidentialité et la sécurité des données transmises. Cependant, l'avocat général Saugmandsgaard Øe a récemment souligné la nécessité pour les responsables du traitement d'assurer la protection des données à caractère personnel, non seulement après leur arrivée dans un pays tiers, mais après que le transfert a été initié, et donc y compris au cours de la phase de transit[57].

Une fois que des données à caractère personnel se trouvent en dehors de l'UE/EEE, en l'absence d'une décision d'adéquation couvrant le pays tiers de destination ou de garanties appropriées, les personnes concernées pourraient également éprouver des difficultés à exercer leurs droits. Dans ces conditions, les droits des personnes concernées, le droit de se plaindre auprès d'une autorité de contrôle indépendante, le droit de demander un recours juridictionnel et le droit de demander réparation, pourraient être concernés.

La Cour a itérativement jugé qu'un contrôle efficace expressément exigé par l'article 8, paragraphe 3, de la Charte, effectué par une autorité indépendante de protection des données est un élément essentiel de la protection des données à caractère personnel[58].

Microsoft et ses sous-traitants ultérieurs risquaient donc de ne pas être suffisamment tenus de rendre compte de leur traitement au titre de l'ILA.

Si les données n'étaient pas traitées dans l'UE/EEE, les institutions de l'UE risquaient également d'avoir de grandes difficultés à faire appliquer le droit de l'UE pour empêcher leur divulgation. En particulier, si les données étaient situées dans un pays tiers, les autorités compétentes du territoire [pouvaient] solliciter l'accès aux données dans le contexte d'une mesure d'application de leur législation publique ou en matière de rétention de données[59].

Dans ce contexte, le CEPD recommande que le traitement des données à caractère personnel confié par les institutions de l'UE à Microsoft ait lieu, en règle générale, au sein de l'UE/EEE.

## 4.5 Recommandations

Le CEPD a recommandé ce qui suit aux institutions de l'UE.

- L'ILA devrait comporter des dispositions présentant de façon détaillée, pour chaque produit et service fourni par Microsoft en vertu de cet accord, la localisation des données collectées et traitées lorsque les institutions de l'UE ont utilisé ce produit ou service spécifique.
- L'ILA devrait explicitement exiger que Microsoft mette en œuvre les garanties contractuelles, organisationnelles et en matière de sécurité appropriées en cas de transfert international de données. En particulier, l'ILA devrait exiger de Microsoft qu'elle mette en place des mesures de sécurité solides pour couvrir les données en cours de transport.
- Tout recours aux CCT pour les transferts devrait être conforme à la législation de l'Union en vigueur.
- L'ILA devrait interdire à Microsoft (et à ses sous-traitants ultérieurs) de communiquer des données à caractère personnel aux autorités des États membres, aux autorités de pays tiers, aux organisations internationales ou à d'autres tiers, à moins que le droit de l'Union ou le droit des États membres ne l'autorise expressément dans la mesure où les conditions prévues par le droit de l'Union pour une telle divulgation sont remplies.
- L'ILA devrait exiger de Microsoft qu'elle informe les institutions de l'UE concernées de toute demande d'accès aux données reçue par elle ou ses sous-traitants, immédiatement à réception de la demande. En règle générale, Microsoft devrait rediriger ces demandes vers l'institution de l'UE concernée et solliciter ses instructions. En tout état de cause, Microsoft devrait contester les demandes d'accès, épuisant toutes les voies de recours disponibles. La divulgation de données par Microsoft ou les sous-traitants ultérieurs ne devrait pas être autorisée sans que l'institution de l'UE concernée ait au préalable été notifiée, ait donné son accord et ses consignes et que les garanties appropriées soient en place. Si une institution de l'UE choisit de ne pas divulguer les données, celles-ci ne devraient être divulguées que sur ordonnance de la Cour de justice de l'Union européenne.
- Outre l'obligation de notification incombant à Microsoft concernant les demandes d'accès aux données, les institutions de l'UE devraient lui demander une fois par an de fournir les informations sur la question de savoir si des données des institutions de l'UE ont été divulguées et,

le cas échéant, quelles mesures, par suite, ont été prises. Les responsables du traitement et leurs délégués à la protection des données pertinents devraient évaluer les informations reçues. Les institutions de l'UE devraient alors prendre toutes les mesures supplémentaires nécessaires pour garantir le respect de l'interdiction contractuelle de divulgation, des procédures de notification et des garanties convenues.

- À moins que les recommandations du CEPD concernant les sous-traitants ultérieurs, la localisation des données, les transferts internationaux et la divulgation non autorisée n'aient été mises en œuvre, l'ILA devrait exiger que tout traitement de données à caractère personnel confié à Microsoft ou à ses sous-traitants par les institutions de l'UE ait lieu, en règle générale, au sein de l'UE/EEE. Cette exigence devrait couvrir le traitement aux fins de la sauvegarde des données, de la continuité des activités et de la réalisation d'opérations à distance.
- À moyen terme, si les institutions de l'UE souhaitaient maintenir les protections prévues par le protocole nº 7 du TFUE et le règlement (UE) 2018/1725 contre toute divulgation non autorisée, elles devraient sérieusement envisager:
    - premièrement, de veiller à ce que les données traitées pour leur compte soient situées dans l'UE/EEE; et
    - deuxièmement, de n'utiliser que des prestataires de services qui ne sont pas assujettis aux lois de pays tiers incompatibles ayant une portée extraterritoriale.

# 5 Mesures techniques

## 5.1 Contexte

En 2016, la Commission a mis en évidence une question de sécurité et de protection des données que posait la collecte par Microsoft de données diagnostiques à partir de ses logiciels. Les logiciels concernés étaient principalement Office Pro Plus 2016 et *Windows 10 Enterprise*. Ces logiciels n'offraient pas de moyens intégrés permettant aux institutions de l'UE de gérer ou de stopper complètement les flux de données diagnostiques vers Microsoft.

Les travaux de la Commission visant à détecter et à atténuer les problèmes liés à la sécurité et à la protection des données posées par les logiciels Microsoft illustraient le fait que, sur un plan technique (donc pas seulement contractuel), l'approche de Microsoft pour fournir ses produits et ses services n'était pas pleinement conforme aux principes de la protection des données dès la conception et par défaut[60].

Les responsables du traitement sont tenus de mettre en œuvre des mesures techniques et organisationnelles pour s'assurer de la protection des données dès la conception et par défaut et de respecter leur obligation de rendre compte[61]. Le CEPD a publié des lignes directrices à l'intention des institutions de l'UE afin de les aider dans ce sens[62].

D'une manière générale, le CEPD recommande que les responsables du traitement évaluent également la nécessité d'apprécier les risques liés à la protection des données lorsqu'ils envisagent d'utiliser des produits ou des services offerts par des prestataires tiers, qui traiteront de grandes quantités de données à caractère personnel.

## 5.2 Recommandations

Dans le contexte particulier de l'ILA et des produits et services que les institutions de l'UE utilisaient au moment de l'enquête, le CEPD a émis les recommandations suivantes.

- En suivant une approche globale et documentée, toutes les institutions de l'UE devraient effectuer des tests pour vérifier le flux de données à caractère personnel vers Microsoft à partir de ses produits et services actuels et futurs. Cette approche devrait notamment:
    - couvrir les modes d'utilisation normaux de leurs utilisateurs impliquant les produits et services de Microsoft à tester;
    - analyser tout flux sortant des ordinateurs de l'utilisateur et toutes ses destinations de manière à distinguer les flux de données circulant depuis les logiciels Microsoft vers les serveurs de Microsoft ou de ses sous-traitants.
- Les institutions de l'UE devraient également surveiller les mises à jour des produits de Microsoft et prendre contact avec la société en vue de

leur configuration afin d'éliminer tout transfert illicite de données à caractère personnel.

- Lorsqu'une institution de l'UE négocie l'acquisition de produits ou de services logiciels pour le compte d'autres institutions de l'UE, l'institution de l'UE réalisant la négociation devrait informer l'autre institution de l'UE de tout problème de protection des données qu'elle décèle avec les produits ou services.
- Les institutions de l'UE devraient partager entre elles l'expertise technique et les solutions afin d'éliminer tout transfert illicite de données à caractère personnel à Microsoft.
- Lorsque les institutions de l'UE ont prévu d'utiliser des produits et services de Microsoft qu'elles n'utilisaient pas encore (tels que Microsoft Office 365 ou les services en nuage Microsoft Azure), elles devraient procéder à des évaluations approfondies des risques liés à la protection des données que présentent ces produits et services avant de les déployer.

# 6 Transparence

L'abondance des documents contractuels, les chevauchements et les conflits de clauses, l'absence de hiérarchie claire et les mises à jour mensuelles rendent, à tout le moins, difficile pour les institutions, organes et organismes de l'UE de s'acquitter de leurs obligations d'information envers les personnes concernées, comme l'exige l'**article 4, paragraphe 1, point a), du règlement (UE) 2018/1725** [*voir également l'article 5, paragraphe 1, point a), du RGPD*].

## 6.1 Recommandations

Dans le contexte particulier de la transparence à l'égard des personnes concernées, qui permet à celles-ci d'exercer leurs droits en matière de protection des données et d'autres droits, le CEPD a émis les recommandations suivantes.

- Obtenir un niveau d'assurance suffisant en ce qui concerne l'objet et la durée du traitement, la nature et les finalités du traitement, les

catégories de données à caractère personnel et de personnes concernées, et les risques pour les personnes concernées afin de permettre aux institutions de l'UE de s'acquitter de leurs obligations de transparence.

- Établir une notice relative à la protection des données dans le cadre des informations devant être fournies aux personnes concernées conformément aux articles 15 et 16 du règlement (UE) 2018/1725.

# 7 Conclusion

Le CEPD recommande aux organisations de ne pas envisager d'engager un sous-traitant (ou sous-traitant ultérieur) qui n'est pas disposé à fournir des garanties suffisantes pour mettre en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences des règles de l'UE en matière de protection des données et garantisse la protection des droits des personnes concernées. Afin de respecter le principe de la protection des données dès la conception et par défaut, les organisations devraient vérifier, tant au moment de la planification du traitement que de sa mise en œuvre, si aucune autre solution logicielle ne permet de renforcer les garanties en matière de protection de la vie privée.

Le CEPD reconnaît que la ligne de conduite recommandée aux institutions de l'UE peut représenter une tâche difficile pour bon nombre, voire pour la plupart, des clients de Microsoft en matière de licences en volume.

Les responsables du traitement dans les institutions de l'UE craignaient certainement qu'un prestataire de services hyper-échelle ne considère les modifications contractuelles, telles que celles que le CEPD préconisait, comme étant soit contraires au bon sens commercial soit irréalisables ou les deux. Le CEPD a constaté que Microsoft s'est montrée, dans une certaine mesure, prête à accepter certaines solutions pour répondre aux besoins des institutions de l'UE en matière de conformité.

Lorsqu'un contractant est véritablement attaché à la protection des données, il apparaît tout à fait possible de renforcer la protection des personnes concernées d'une manière qui soit commercialement acceptable et qui puisse admettre de nombreux clients en même temps.

Par conséquent, le CEPD exhorte les responsables du traitement à ne pas se décourager à la perspective de négocier avec un sous-traitant des instructions qu'ils jugent nécessaires pour protéger les droits et les libertés des personnes concernées, même lorsqu'ils sont face à un partenaire commercial d'une envergure considérable.

---

1. ↩ Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, JO L 295 du 23.10.2018, p. 60.↩
2. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1.↩
3. Le CEPD respecte ce niveau élevé de transparence en vue de mieux faire connaître les questions liées à la protection des données, en favorisant une compréhension commune des règles de protection des données et le développement de la culture de la protection des données dans l'ensemble de l'UE/EEE. Un niveau élevé de transparence est généralement recommandé par le Médiateur européen pour les institutions de l'UE en ce qui concerne la mise en œuvre proactive du règlement (CE) nº 1049/2001 et la responsabilité du processus décisionnel de l'UE.↩
4. Règlement (UE) 2018/1725.↩
5. RGPD.↩
6. Le rôle et les compétences du CEPD concernent uniquement le respect du règlement (UE) 2018/1725 et non du RGPD. Afin d'aider les lecteurs, lorsque le présent document fait référence à des dispositions spécifiques du règlement (UE) 2018/1725, les références aux dispositions correspondantes du RGPD ont été ajoutées.↩
7. Règlement (UE) 2018/1725, considérant 48 et article 25.↩

8. «Conditions d'octroi de la licence et documentation» (*Contrats de licence en volume de Microsoft*) <https://aka.ms/licensingdocs>.↩
9. Microsoft, «Introduction», *Conditions relatives aux services en ligne* <https://aka.ms/ost>, partie «Conditions du DPA et mises à jour applicables»; Microsoft, «Introduction», *Addendum sur la protection des données* <https://aka.ms/dpa>, partie «Conditions du DPA et mises à jour applicables».↩
10. Idem.↩
11. Au moment de la rédaction du présent document (mai 2020), la dernière version de l'*addendum sur la protection des données* était celle de janvier 2020.↩
12. Les versions antérieures et postérieures à janvier 2020 peuvent présenter un intérêt pour les institutions de l'UE.↩
13. Règlement (UE) 2018/1725, article 29, paragraphe 10; RGPD, article 28, paragraphe 10.↩
14. Microsoft, «Conditions de protection des données», *Addendum sur la protection des données* <https://aka.ms/dpa>, sous-partie «Rôles et responsabilités du sous-traitant et du responsable du traitement»; Microsoft, «Annexe 1», *Addendum sur la protection des données* <https://aka.ms/dpa>, sous-partie «Rôles et responsabilités du sous-traitant et du responsable du traitement».↩
15. «Avis 03/2013 sur la limitation des finalités» (Groupe de travail «Article 29», 2012) p. 15 et 16 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>; «Lignes directrices 2/2019 sur le traitement des données à caractère personnel au titre de l'article 6, paragraphe 1, point b), du RGPD dans le cadre de la fourniture de services en ligne aux personnes concernées» (Comité européen de la protection des données 2019) p. 6 et 7<https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_fr.pdf'>.↩
16. Microsoft, «Conditions de protection des données dans l'addendum sur la protection des données» (note 14), sous-partie «Traitement pour fournir au client les services professionnels».↩
17. Idem.↩

18. Idem.↩

19. Idem.↩

20. Privacy Company, «DPIA Diagnostic Data in Microsoft Office Proplus» [Ministry of Justice and Security for the benefit of SLM Rijk (Strategic Vendor Management Microsoft Dutch Government), 2018] p. 37. <https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office/DPIA+Microsoft+Office+2016+and+365+-+20191105.pdf>.↩

21. Microsoft, «Conditions de protection des données dans l'addendum sur la protection des données» (note 14), sous-partie «Traitement pour les besoins professionnels légitimes de Microsoft».↩

22. RGPD, article 28, paragraphe 3.↩

23. Idem, article 28, paragraphe 3.↩

24. Idem, article 28, paragraphe 3.↩

25. Règlement (UE) 2018/1725, article 29, paragraphe 1; RGPD, article 28, paragraphe 1.↩

26. Règlement (UE) 2018/1725, article 29, paragraphe 2; RGPD, article 28, paragraphe 2.↩

27. Règlement (UE) 2018/1725, article 29, paragraphe 2; article 28, paragraphe 2 du RGPD; dans ce contexte également, il convient de citer l'«avis 14/2019 sur le projet de clauses contractuelles types présenté par l'autorité de contrôle du Danemark (article 28, paragraphe 8, du RGPD)» (Comité européen de la protection des données, 2019), paragraphe 29. <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_201914_dk_scc_fr.pdf>.↩

28. Règlement (UE) 2018/1725, article 29, paragraphe 4; RGPD, article 28, paragraphe 4.↩

29. Règlement (UE) 2018/1725, article 29, paragraphe 4; RGPD, article 28, paragraphe 4.↩

30. Règlement (UE) 2018/1725, article 26; RGPD, article 24.↩

31. La conception du CEPD repose sur les informations disponibles sur: «Trust Center» (*Microsoft*) https://www.microsoft.com/fr-ww/trust-center>.↩

32. Règlement (UE) 2018/1725, article 29, paragraphe 4; RGPD, article 28, paragraphe 4.↩

33. Voir également l'article 28, paragraphe 3, point 2, du RGPD.↩

34. Voir également l'article 28, paragraphe 3, du RGPD.↩

35. Voir la section intitulée «Champ d'application» de l'*addendum sur la protection des données*, qui exclut les services en ligne mentionnés en son annexe 1 (à savoir les services professionnels) du champ d'application dudit addendum. Voir également la sous-partie «Champ d'application» de la section «Conditions de protection des données» dans les versions 2019 des conditions relatives aux services en ligne.↩

36. Voir «Annexe 1» dans les *Conditions relatives aux services en ligne*. Voir également la sous-partie «Champ d'application» de la section «Conditions de protection des données» dans les versions 2019 des *Conditions relatives aux services en ligne*.↩

37. Voir Microsoft, «Conditions de protection des données de l'addendum sur la protection des données» (note 14), sous-partie «Respect des audits», lue dans son ensemble.↩

38. Voir également l'article 28, paragraphe 3, point h), du RGPD.↩

39. Microsoft, «Conditions de protection des données de l'addendum sur la protection des données» (note 14), sous-partie «Respect des audits».↩

40. Microsoft, «Annexe 1», *Conditions relatives aux services en ligne* <https://aka.ms/ost> partie «Emplacement des données client au repos pour les services en ligne Core».↩

41. Idem.↩

42. Idem.↩

43. Microsoft, «Conditions de protection des données de l'addendum sur la protection des données» (note 14), partie «Transferts et emplacement des données», sous-partie «Transferts des données».↩

44. «Déclaration de confidentialité» ( *Microsoft*) < https://aka.ms/privacy>, partie «Où nous conservons et traitons les données à caractère personnel».↩

45. Règlement (UE) 2018/1725, chapitre V, en particulier article 46; chapitre V et notamment article 44, du RGPD.↩

46. Microsoft, «Annexe 2», «*Addendum sur la protection des données*» <https://aka.ms/dpa>.↩

47. Voir également article 46, paragraphe 2, points c) et d), du RGPD.↩

48. «Lettre à Microsoft concernant une nouvelle version de l'accord sur le traitement des données issues de services en ligne Microsoft dans le cadre de l'addendum sur l'inscription des entreprises et son annexe I» (Groupe de travail «Article 29», 2014) < https://ec.europa.eu/justice/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf>.↩

49. Microsoft, «Addendum sur la protection des données Annexe 2» (note 46) annexes 1 et 2.↩

50. Voir, à cet égard, les «Lignes directrices sur l'utilisation des services d'informatique en nuage par les institutions et organes de l'Union européenne» (CEPD 2018), paragraphe 60. <https://edps.europa.eu/sites/edp/files/publication/18-03-16_cloud_computing_guidelines_fr.pdf>.↩

51. «Réponse conjointe à la commission LIBE concernant l'incidence du Cloud Act américain sur le cadre juridique européen en matière de protection des données à caractère personnel» (EDPB; CEPD 2019).<https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en>.↩

52. Voir également l'article 5, paragraphe 1, point f) du RGPD.↩

53. Microsoft, «Conditions de protection des données de l'addendum sur la protection des données» (note 14), «Divulgation des données traitées».↩

54. Idem, «Divulgation des données traitées» ou «Divulgation des données client ou des données à caractère personnel» dans les versions antérieures à 2020.↩

55. «Déclaration de confidentialité» (note 44), partie «Raisons pour lesquelles nous partageons vos données personnelles», «Où nous stockons et traitons les données» et «Skype - sociétés partenaires». Les données susceptibles d'être divulguées comprennent les «données clients», les «données d'administrateur», les «données de paiement» et les «données de support».↩

56. Conclusions de l'avocat général Saugmandsgaard Øe présentées le 19 décembre 2019 dans l'affaire C-311/18, Data Protection Commissioner/Facebook Ireland Limited et Maximillian Schrems, EU:C:2019:1145, [2018] JO C 249/21, points 1 et 204.↩

57. Idem, points 234 à 237.↩

58. Arrêt de la Cour du 16 octobre 2012, Commission/Autriche, C-614/10, EU:C:2012:631, JO C 72/13, point 37; arrêt de la Cour du 8 avril 2014 dans les affaires jointes Digital Rights Ireland Ltd/Ministère de la marine, des ressources naturelles et autres et Kärntner Landesregierung et autres, C-293/12–C-594/12, EU:C:2014:238, point 68; arrêt de la Cour du 6 octobre 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, EU:C:2015:650, point 41.↩

59. «Lignes directrices sur l'utilisation de services d'informatique en nuage par les institutions et les organes de l'Union européenne», «Lignes directrices du CEPD sur l'informatique en nuage» (n 50), point 63.↩

60. Règlement (UE) 2018/1725, article 27; RGPD, article 25.↩

61. Règlement (UE) 2018/1725, articles 26 et 27; RGPD, articles 24 et 25.↩

62. Lignes directrices sur la protection des données à caractère personnel pour la gouvernance informatique et la gestion informatique des institutions européennes (CEPD 2018). <https://edps.europa.eu/sites/edp/files/publication/it_governance_management_fr.pdf>; «Lignes directrices sur l'utilisation des services d'informatique en nuage par les institutions et les organes de l'Union européenne», «Lignes directrices du CEPD pour l'informatique en nuage» (note 50).↩

# Impression

Luxembourg: Office des publications de l'Union européenne, 2020

| | | | |
|---|---|---|---|
| PDF | ISBN 978-92-9242-567-8 | doi:10.2804/14519 | QT-03-20-457-EN-N |
| EPUB | ISBN 978-92-9242-565-4 | doi:10.2804/215182 | QT-03-20-457-EN-E |
| HTML | ISBN 978-92-9242-566-1 | doi:10.2804/300986 | QT-03-20-457-EN-Q |