EUROPEAN DATA PROTECTION SUPERVISOR

Lignes directrices sur l'utilisation des services d'informatique en nuage par les institutions et les organes de l'Union européenne

16 mars 2018

TABLE DES MATIÈRES

Objectif et champ d'application

Les institutions, organes et agences de l'Union européenne (ci-après les «institutions de l'UE») envisagent l'utilisation des services informatiques en nuage en raison des avantages qu'ils présentent, tels que la réduction des coûts et les gains de flexibilité. Elles sont toutefois confrontées aux risques spécifiques que comporte le paradigme de l'informatique en nuage et doivent assumer l'ensemble de la responsabilité à l'égard de leurs obligations en matière de protection des données. En ce qui concerne les services en nuage, les institutions de l'UE devraient garantir un niveau de protection des données à caractère personnel équivalent à tout autre type de modèle d'infrastructure de TI.

Les présentes lignes directrices ont pour objectif de fournir **des instructions et des conseils pratiques** aux institutions de l'UE afin que celles-ci respectent le règlement (CE) nº 45/2001. Étant donné qu'un processus législatif est en cours dans le but d'intégrer les principes du règlement général sur la protection des données [règlement (UE) 2016/679, ci-après le «RGPD»] dans les règles en matière de protection des données pour les institutions de l'UE, il est tenu compte des nouveaux concepts dans les présentes lignes directrices, en se référant aux dispositions pertinentes du RGPD. Après l'adoption du nouveau règlement sur la protection des données pour les institutions de l'UE, une version mise à jour sera publiée.

Les présentes lignes directrices fournissent des recommandations et indiquent les bonnes pratiques visant à mettre en œuvre la responsabilité de la protection des données à caractère personnel en **aidant à évaluer et à gérer les risques relatifs à la protection des données, à la vie privée et à d'autres droits fondamentaux des individus dont les données à caractère personnel sont traitées à l'aide de services en nuage**. Elles rassemblent et consolident les conseils que le contrôleur européen de la protection des données (CEPD) a prodigués aux institutions de l'UE ces dernières années, concernant les premiers appels d'offres interinstitutionnels par exemple.

Les présentes lignes directrices indiquent l'approche que les institutions de l'UE devraient adopter pour protéger de manière adéquate les données à caractère personnel au moment d'envisager la possibilité de recourir à des services d'informatique en nuage pour leurs systèmes de TI. Les risques spécifiques que présente le modèle d'informatique en nuage, qui inclut et, souvent, amplifie les risques liés à l'externalisation des services, doivent être recensés et gérés, et des garanties pertinentes doivent être mises en place.

Le CEPD considère les bonnes pratiques mentionnées ci-après comme **une référence** lors de l'analyse du respect du règlement. Les institutions de l'UE peuvent choisir d'autres mesures, également efficaces, que celles présentées dans le présent document, en fonction de leurs besoins spécifiques. Dans ce cas, elles devront démontrer de quelle manière ces mesures entraînent une protection équivalente des données à caractère personnel.

Si les présentes lignes directrices sont destinées aux DPD, aux CPD, au personnel des services des TI et de la sécurité des TI ainsi qu'aux autres services administratifs des institutions de l'UE participant à la conception, à la planification et à l'attribution des services informatiques en nuage, elles peuvent également se révéler utiles aux autres organisations intéressées par la protection des données et l'informatique en nuage.

Dans le cadre de la protection des données, les institutions de l'UE doivent analyser l'impact des services en nuage planifiés sur les données qui seront traitées. Si l'analyse indique que l'institution de l'UE peut, en principe, adopter des garanties pour réduire les risques à un niveau acceptable, alors cette institution doit tenir compte des exigences qui en résultent et les utiliser comme contribution dans le cahier des charges des marchés publics. Si le résultat de l'évaluation est négatif, les institutions de l'UE devraient modifier leurs plans et soit envisager des services d'informatique en nuage moins risqués, soit abandonner l'ensemble de l'option en nuage.

Les lignes directrices sont axées sur:

- l'évaluation du caractère approprié de l'option d'informatique en nuage;

- la manière dont les exigences en matière de protection des données doivent être prises en considération au moment de déterminer et de choisir l'option d'informatique en nuage dans le processus de passation de marchés publics;
- une référence en matière de garanties techniques et organisationnelles pertinentes, mettant l'accent sur les clauses contractuelles.

L'identification et l'évaluation des principaux risques spécifiques au nuage sont présentées dans une annexe.

L'accent est mis en particulier sur les contrats de fourniture de services d'informatique en nuage. Des orientations sont également données concernant l'exploitation des services en nuage et des accords de niveau de service (ANS), qui peuvent également servir à décrire les exigences en matière de sécurité des TI. Les accords contractuels devraient également intégrer les modalités de résiliation des contrats de services, y compris la restitution des données sans complication ou la portabilité vers un autre fournisseur de services.

1. Introduction

1 Les institutions, organes et agences de l'Union européenne (ci-après les «institutions de l'UE») envisagent l'utilisation des services d'informatique en nuage en raison des avantages qu'ils présentent, tels que la réduction des coûts initiaux et des coûts de gestion et l'externalisation partielle ou complète des applications logicielles, de l'infrastructure des TI[1] et du stockage de données. L'informatique en nuage permettrait de réduire ou d'éviter les efforts et les tâches internes liés à la gestion des TI et créera de nouvelles capacités ainsi que, dans certaines circonstances, plusieurs avantages, tels qu'un niveau d'assurance plus élevé concernant la sécurité des TI. Les institutions de l'UE sont toutefois confrontées aux risques spécifiques que comporte le paradigme de l'informatique en nuage et doivent assumer l'ensemble de la responsabilité à l'égard de leurs obligations en matière de protection des données.

2 Les présentes lignes directrices ont pour objectif de fournir des instructions et des conseils pratiques aux institutions de l'UE afin que celles-ci respectent le règlement (CE) nº 45/2001[2] et la proposition de révision y afférente (ci-après la «proposition de règlement»)[3], en les aidant dans l'analyse et la gestion des risques liés à la protection des données, à la vie privée et à d'autres droits fondamentaux des individus dont les données à caractère personnel sont traitées à l'aide de services en nuage. Elles rassemblent et consolident les conseils que le contrôleur européen de la protection des données (CEPD) a prodigués aux institutions de l'UE ces dernières années.

3 Les principes de la proposition de règlement devraient être les mêmes que ceux du nouveau règlement général sur la protection des données [règlement (UE) 2016/679, ci-après le «RGPD»][4] applicable dans les États membres de l'UE et de l'EEE. En attendant l'approbation de la proposition de règlement, **les présentes lignes directrices font référence aux dispositions du RGPD lorsque des articles spécifiques sont mentionnés. Le texte sera mis à jour une fois la proposition de règlement adoptée et publiée.**

4 En tant qu'autorité de contrôle indépendante compétente pour le traitement des données à caractère personnel par les institutions de l'UE, le CEPD peut, entre autres, publier des lignes directrices sur des questions spécifiques relatives au traitement des données à caractère personnel. Les présentes lignes directrices sont le fruit d'un processus au cours

---

[1] Le terme «TI» désigne les technologies de l'information et de la communication.

[2] Règlement (CE) nº 45/2001 du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1).

[3] Proposition de règlement du Parlement européen et du Conseil 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, COM(2017) 8 final du 10.1.2017, disponible à l'adresse: http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=COM:2017:0008:FIN

[4] 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, disponible à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L:2016:119:FULL.

duquel les institutions de l'UE ont été consultées et ont fait part de leurs observations au CEPD[5].

5 Les présentes lignes directrices sont destinées aux délégués à la protection des données (DPD) et aux coordinateurs de la protection des données (CPD) au sein de chaque institution de l'UE, ainsi qu'au personnel des TI et de la sécurité des TI et aux autres services administratifs participant à la conception, à la planification et à l'attribution de services informatiques en nuage.

6 L'objectif des lignes directrices est d'aider les institutions de l'UE à remplir leurs obligations. Ces institutions restent toutefois responsables du respect de ces obligations conformément au principe de responsabilité. Les mesures recommandées dans les présentes lignes directrices permettent aux institutions de l'UE de commencer à appliquer ce qui est attendu de leur part concernant la responsabilité et se veulent prospectives, car elles tiennent compte des changements législatifs attendus. Les institutions de l'UE peuvent choisir d'autres mesures, également efficaces, que celles présentées dans le présent document, en fonction de leurs besoins spécifiques. Dans ce cas, elles devront démontrer de quelle manière elles entendent obtenir une protection équivalente des données à caractère personnel à l'aide de ces autres mesures.

[5] En 2017, le CEPD a transmis un projet de ces lignes directrices aux délégués à la protection des données ainsi qu'aux agents chargés de la sécurité des TI et aux gestionnaires des TI des institutions, organes et agences de l'UE. Environ 400 commentaires ont été reçus et pris en considération dans la version finale.

2. Champ d'application et structure des lignes directrices

7 Le présent document explique aux institutions de l'UE comment protéger les données à caractère personnel et la vie privée et comment respecter la proposition de règlement lors de la planification et de l'utilisation des services d'informatique en nuage dans le cadre de leurs tâches institutionnelles, ce qui répond aux besoins opérationnels qu'elles ont exprimés dans les demandes de consultations et de vérifications préalables gérées par le CEPD.

8 Le présent document est axé sur l'utilisation des services d'informatique en nuage fournis par des entités commerciales. À cet effet, il aborde également tout naturellement la question de l'externalisation des services de TI qui traitent des données à caractère personnel.

9 Les lignes directrices portent, en particulier, sur:

- **les rôles et responsabilités en matière de protection des données** des institutions de l'UE et du fournisseur de services en nuage, ainsi que les aspects liés à leur responsabilité (section 3);
- les facteurs dont il faut tenir compte lors de l'**évaluation** et de la **sélection** d'un service d'informatique en nuage au moyen d'un marché public, y compris la **façon de l'aborder** et les **garanties** pertinentes (sections 4.1et 4.2);
- le fonctionnement des services d'informatique en nuage et les dispositions/garanties à assurer pour la «fin du contrat» (section 4.3);
- des exemples de **contrôles de sécurité** qui atténuent les risques spécifiques au nuage (section 4.4) et des références à des sources externes (voir Annexe 5) pour traiter le sujet plus en profondeur.

10 Les informations suivantes sont fournies en annexe pour appuyer les orientations:

- des orientations juridiques supplémentaires concernant des questions spécifiques (Annexe 2);
- des concepts de base de l'informatique en nuage, les aspects spécifiques du modèle de service (IaaS/ PaaS/ SaaS) et du modèle de déploiement (public, privé, communautaire ou hybride) des environnements en nuage (Annexe 3);
- une description des risques spécifiques à la protection des données créés ou amplifiés par l'utilisation de services informatiques en nuage (Annexe 4);
- des références à d'autres documents utiles (avis, normes techniques, bonnes pratiques, etc.) (Annexe 5).

11 Ce document ne traite pas/ne tient pas compte:

- des risques pour les institutions de l'UE posés par l'informatique en nuage qui n'ont pas trait au respect de la proposition de règlement, comme les risques financiers liés à l'acquisition de services en nuage ou aux informations confidentielles;
- des risques liés à la sécurité des TI qui ne sont pas particulièrement provoqués ou amplifiés par des services informatiques en nuage;
- d'une couverture exhaustive des mesures pertinentes en matière de sécurité des TI;
- des caractéristiques techniques et fonctionnelles de l'infrastructure des TI fournie, comme le type de serveurs, les applications et les plateformes logicielles, les dispositifs réseaux, etc.;

- des obligations et principes fondamentaux en matière de protection des données, sauf s'ils sont spécifiquement touchés par l'utilisation des services d'informatique en nuage. Des orientations adéquates à ce sujet sont fournies par d'autres produits existants ou prévus du CEPD.

3. Aborder l'option de l'informatique en nuage

3.1. Garantir un niveau de protection des données à caractère personnel équivalent à tout autre type de modèle informatique

12 Le recours à des services informatiques en nuage peut comporter des avantages, dans certaines circonstances, notamment l'augmentation du niveau de protection des informations traitées. Toutefois, le modèle informatique en nuage comporte aussi de nouveaux risques[6] pour les données à caractère personnel et modifie le niveau des risques existants. Parmi les principaux problèmes dans ce domaine figure le fait que, dans le modèle informatique en nuage, les organisations et les particuliers ont généralement moins de contrôle sur la manière dont les données sont traitées et exploitées; de nombreux tiers peuvent contribuer à l'offre de service, ce qui génère de l'incertitude quant à la responsabilité de chacun; l'utilisation de l'internet public ajoute un élément de risque et l'interaction dynamique de nombreux centres de données fournit moins d'assurance concernant la localisation physique des données.

13 Le principe sous-jacent essentiel des présentes lignes directrices est que l'informatique en nuage ne devrait pas diminuer le niveau de protection des données à caractère personnel par rapport au traitement des données effectué à l'aide d'un autre modèle d'infrastructure de TI[7].

Par exemple, le traitement des données à caractère personnel à l'aide d'un service en nuage ne doit pas entraîner de périodes de conservation différentes de celles fixées pour le traitement «hors nuage» par les lignes directrices thématiques pertinentes du CEPD[8].

14 Par conséquent, des **garanties spécifiques[9] sont nécessaires pour faire face aux risques émergents** afin que le niveau de protection soit équivalent. Si des garanties adéquates ne sont pas disponibles, les institutions devraient modifier leurs plans et envisager des services information en nuage moins risqués ou abandonner l'ensemble de l'option en nuage.

---

[6]Voir Annexe 4 qui recense les risques élevés liés à la protection des données que comportent les services informatiques en nuage.

[7] «Protocole d'accord de Sopot», adopté en avril 2012 par le groupe de Berlin ou groupe de travail international sur la protection des données dans les télécommunications (IWGDPT), disponible à l'adresse:

https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=3065.

Voir la résolution du Parlement européen du 10 décembre 2013 sur l'informatique en nuage, recommandation, «63. [...] en règle générale, **le niveau de protection des données dans un environnement d'informatique en nuage ne doit pas être inférieur au niveau exigé dans tout autre contexte de traitement de données**». Dans la même veine, voir la résolution du Parlement européen du 12 mars 2014: «considérant que le niveau de protection des données dans un environnement d'informatique en nuage ne doit pas être moins élevé à celui exigé dans un autre cadre de traitement de données; que le droit de l'Union en matière de protection des données, neutre sur le plan technologique, s'applique déjà pleinement aux services d'informatique en nuage actifs dans l'Union européenne».

[8] À titre d'exemple, le CEPD a publié des lignes directrices concernant le traitement des données à caractère personnel en matière de congé et d'horaire flexible; elles sont disponibles sur le site web du CEPD:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/12-12-20_Guidelines_Leave_Flexitime_FR.pdf; les périodes de conservation des données sont précisées aux pages 9 à 11.

[9] Les termes «garanties», plus fréquent dans le domaine de la protection des données, et «contrôle», plus fréquent dans le domaine de la sécurité des TI, désignent tous deux les mesures utilisées pour faire face aux risques.

15 Les conseils stratégiques prodigués précédemment par le CEPD et le groupe de travail «Article 29»[10] peuvent être utiles pour analyser les défis présentés par l'informatique en nuage et pour planifier les garanties adéquates.

3.2. Gouvernance et responsabilité: garder le contrôle sur le traitement des données dans un contexte en nuage

16 Même si les institutions de l'UE assument le rôle du **responsable du traitement** et que le fournisseur de services en nuage n'est généralement que le **sous-traitant**[11], les **rôles et les responsabilités** respectifs de toutes les parties doivent être clairement définis. Le rôle du fournisseur de services n'est pas toujours clair pour de nombreux services d'informatique en nuage sur le marché. Parfois, les fournisseurs de services en nuage gardent un niveau de contrôle sur le traitement qui dépasse le cadre du rôle de sous-traitant en menant des opérations sur des données à caractère personnel qui n'ont pas été demandées par le client ou en ne laissant pas suffisamment le choix au client en ce qui concerne les procédures ou les moyens de traitement. Les institutions de l'UE doivent éviter que cela se produise en négociant des garanties et des contrats adaptés ou en choisissant un autre fournisseur de services en nuage.

17 Les institutions de l'UE, en raison des obligations juridiques qui leur incombent[12], doivent **garder le contrôle** (en déterminant les **finalités** et les **moyens**) du traitement des données à caractère personnel effectué à l'aide du service en nuage. Des dispositions spécifiques doivent être intégrées dans le cadre juridique contractuel entre l'institution de l'UE et le fournisseur de services en nuage (le «contrat») à cette fin.

---

[10] Concernant les défis posés par l'informatique en nuage par rapport à la protection des données, voir l'avis du contrôleur européen de la protection des données relatif à la communication de la Commission intitulée «Exploiter le potentiel de l'informatique en nuage en Europe», disponible à l'adresse:

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_FR.pdf.

et l'avis 05/2012 du groupe de travail «Article 29» sur l'informatique en nuage, disponible à l'adresse suivante:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf

[11] Conformément à la définition prévue à l'article 2 du règlement (CE) nº 45/2001 et à l'article 4, paragraphe 8, du RGPD.

[12] Par exemple, conformément à l'article 14 du règlement (CE) nº 45/2001, la personne concernée a le droit d'obtenir *du responsable du traitement* [qui est défini à l'article 2, point d), dudit règlement comme étant «l'institution ou organe communautaire, la direction générale, l'unité ou toute autre entité organisationnelle»] la rectification de données à caractère personnel inexactes ou incomplètes.

Voir également l'article 23, paragraphe 2, point a), du règlement, qui énonce que «le sous-traitant n'agit que sur instruction du responsable du traitement».

En vertu du RGPD, l'article 16 prévoit également: «La personne concernée a le droit d'obtenir *du responsable du traitement*, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes.» Tout comme le règlement (CE) nº 45/2001, l'article 28, paragraphe 3, du RGPD prévoit que «le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement».

18 En résumé, pour **garder le contrôle** afin de garantir la conformité totale à la proposition de règlement[13] et pour se montrer responsables, les institutions de l'UE doivent:

- **sélectionner un fournisseur de services en nuage qui donne des garanties suffisantes** concernant les mesures techniques et non techniques qu'il peut mettre en œuvre pour aider l'institution de l'UE à respecter et garantir les droits en matière de protection des données des personnes dont les données sont traitées;
- **conclure un contrat juridiquement contraignant[14] (le «contrat») entre elles et le fournisseur de services en nuage** et établir, entre autres conditions, que le «client en nuage» (l'institution de l'UE) est l'**unique responsable du traitement** et que le sous-traitant ne doit pas traiter les données sans instructions du responsable du traitement;
- une fois le contrat opérationnel, il convient de **garantir et de contrôler activement la mise en œuvre** des garanties et des autres dispositions contractuelles requises.

19 Il convient de rappeler que, en tant que **sous-traitant**, le fournisseur de services en nuage est juridiquement soumis à des **obligations spécifiques** et se montre responsable vis-à-vis de celles-ci (articles 28, 29 et 30 du RGPD[15]).

20 Le fournisseur de services en nuage **doit assister** l'institution de l'UE pour veiller au respect des obligations en matière de protection des données, en particulier concernant les réponses rapides de ces institutions aux demandes d'accès, de verrouillage, de rectification ou de suppression des données des personnes concernées exerçant leurs **droits en matière de protection des données[16]**. Le contrat doit préciser si le responsable du traitement doit avoir un contrôle direct dans la réalisation des opérations de traitement nécessaires pour mettre en œuvre les droits des personnes concernées ou si le fournisseur de services en nuage doit réagir rapidement à toute instruction donnée par l'institution de l'UE pour mettre en œuvre une demande d'une personne concernée (visant à accéder, rectifier, verrouiller ou supprimer des données à caractère personnel). En tout état de cause, il doit être clairement indiqué que la réponse finale à la personne concernée doit être apportée par l'institution de l'UE ou selon ses instructions.

3.3. Planification des marchés publics pour les services informatiques en nuage

21 Compte tenu des considérations qui précèdent et au vu de la nature juridique, des tâches et des responsabilités institutionnelles (l'exercice d'une fonction publique, ce qui entraîne des

---

[13] Il convient de rappeler que des dispositions spécifiques du RGPD sur le traitement des données à caractère personnel au nom des institutions et organes de l'UE (au titre de l'article 28) s'appliquent dans ce cas.

[14] Le terme «contrat» désigne **à la fois** le contrat *et* l'accord de niveau de service, ainsi que toutes les annexes, qui forment ensemble le cadre contractuel prévu par l'institution de l'UE avec le fournisseur de services en nuage.

Ce que le fournisseur de services en nuage doit faire pour aider le responsable du traitement dans la réalisation de ses tâches est défini dans les contrats écrits. Ces contrats sont généralement structurés de façon à ce que les modalités opérationnelles du service rendu par le fournisseur de services en nuage soient définies et convenues dans une section contractuelle ou un document différent, qui serait toujours une extension du contrat (l'accord de niveau de service). Même si, aux fins des présentes lignes directrices, nous suivons le principe selon lequel il existe une différence entre ces deux documents, les institutions de l'UE sont libres d'établir la structure de contrat comme elles le souhaitent.

[15] Voir les articles 28 à 30 du RGPD.

[16] Comme établi aux articles 12 à 23 du RGPD.

précautions particulières) des institutions de l'UE[17], ces dernières devraient suivre le processus suivant lors de la planification des services d'informatique en nuage:

- obtenir les **conseils d'experts** et chercher à adopter de **bonnes pratiques** pertinentes. Établir des liens avec les autres institutions de l'UE pour obtenir une expertise sur les expériences précédentes en matière de passation de marchés publics, par exemple;
- **former** les décideurs, les entrepreneurs, les gestionnaires de contrat et le personnel des services de TI aux risques liés à la protection des données émanant de l'utilisation de services d'informatique en nuage, et demander aux contractants d'être formés;
- réaliser une **analyse des risques en matière de protection des données** afin de vérifier s'il est possible d'acquérir des services en nuage pour faciliter les opérations de traitement des données dans le cadre du champ d'application envisagé et sélectionner un fournisseur de services en nuage approprié qui peut offrir un niveau de protection adéquat des données à caractère personnel en vue de réduire l'incidence sur les libertés et droits fondamentaux des personnes et garantir le respect de la proposition de règlement.

  Le niveau de formalisme et de compréhension de l'analyse peut varier en fonction des facteurs détaillés à la section 4.1.

22 Il est recommandé aux institutions de l'UE de commencer à développer un savoir-faire et de gagner de l'expérience dans le domaine du traitement des données à caractère personnel via des services en nuage pour les opérations comportant **des risques moins importants en matière de protection des données**[18], si possible, et de n'envisager des opérations plus sensibles qu'après avoir été rassurées quant à la capacité à exercer un contrôle efficace sur ces services.

23 Dans le cas où l'option en nuage planifiée est envisageable (sur la base de l'évaluation), l'institution de l'UE doit en particulier:

- déterminer les rôles nécessaires, attribuer les ressources et les tâches pertinentes et mettre en place des politiques, des processus et des procédures internes pour gérer les services en nuage attendus;

---

[17] Les institutions et organes de l'UE constituent une forme spéciale d'administration publique, de niveau supranational, dont le cadre juridique en matière de protection des données est représenté par le règlement (CE) nº 45/2001 et, dans un avenir proche, par la proposition de règlement. Sur le plan juridique, il est important de noter que la législation susmentionnée en matière de protection des données est appliquée **en association avec** d'autres textes législatifs régissant les activités des institutions et organes de l'UE, tels que le **protocole sur les privilèges et immunités de l'Union européenne.**

Protocole (n º36) sur les privilèges et immunités de l'Union européenne (1965), Journal officiel C 321 E du 29.12.2006, p. 318 à 324, disponible à l'adresse:

http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:12012E/PRO/07&from=FR.

Il est également fait référence au protocole sur les privilèges et immunités dans les **règlements instituant les agences de l'UE**, par exemple, le règlement (UE) n º1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), qui prévoit l'article suivant: «Article 67 - Privilèges et immunités: Le protocole (n º7) sur les privilèges et immunités de l'Union européenne annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne s'applique à l'Autorité ainsi qu'à son personnel.»

[18] À l'exception, en principe, des catégories spéciales de données à caractère personnel visées à l'article 9 du RGPD.

- garantir que les contrats et les accords de niveau de service passés avec le fournisseur de services en nuage contiennent toutes les garanties nécessaires, y compris, en particulier:
    - mentionner clairement que le fournisseur de services en nuage traite les données à caractère personnel confiées par l'institution de l'UE **uniquement sur instruction documentée de l'institution de l'UE**;
    - garantir que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la **confidentialité** ou sont soumises à une obligation statutaire de confidentialité appropriée;
    - mentionner et définir clairement les **responsabilités** et les **obligations** des différentes parties (y compris des sous-traitants ultérieurs, le cas échéant);
    - définir et mentionner clairement, en particulier, la manière dont le fournisseur de services en nuage aide l'institution de l'UE dans le cadre du respect de ses obligations en tant que responsable du traitement à l'égard des personnes concernées et du CEPD;
    - prévoir des dispositions octroyant à l'institution de l'UE la capacité de réaliser des **audits** elle-même auprès du fournisseur de services en nuage ou par l'intermédiaire d'un auditeur externe (tiers) mandaté par elle;
    - mentionner clairement la **localisation** du fournisseur de services en nuage et de tout autre sous-traitant engagé par ce fournisseur (sous-traitants ultérieurs), le cas échéant, ainsi que de leurs opérations de traitement des données, y compris des sauvegardes;
    - mentionner clairement que le sous-traitant ne peut engager d'autre **sous-traitant ultérieur** sans l'autorisation écrite préalable de l'institution de l'UE. Cette autorisation peut-être spécifique (pour un sous-traitant ultérieur particulier) ou générale. En cas d'autorisation générale, le fournisseur de services en nuage informe le responsable du traitement si des sous-traitants ultérieurs viennent s'ajouter ou sont remplacés et l'institution de l'UE a le droit de s'opposer à ces changements;
    - **ne pas divulguer** aux autorités répressives des États membres de l'UE ou des pays tiers les données à caractère personnel confiées au fournisseur de services en nuage (ainsi qu'aux sous-traitants ultérieurs, le cas échéant) par l'institution de l'UE, *sauf autorisation expresse dans la législation de l'Union.* En tant qu'organe de l'UE, l'institution de l'UE est soumise aux **privilèges et immunités de l'Union européenne**[19], en particulier en ce qui concerne l'inviolabilité des archives (y compris la localisation physique des services) et la sécurité des informations;
    - posséder des procédures d'élimination/de récupération/de portabilité des données;
    - **supprimer ou restituer**, à la discrétion de l'institution de l'UE, l'ensemble des données à caractère personnel confiées par cette dernière au fournisseur de services en nuage au terme de la fourniture des services;
    - mentionner clairement les **mesures de sécurité des TI** que le fournisseur de services en nuage et tout sous-traitant ultérieur doivent fournir;

[19] Voir la note de bas de page 17.

- gérer le contrat, son exécution et sa résiliation, et garder le contrôle des opérations réalisées par le fournisseur de services en nuage concernant les données à caractère personnel «confiées» par l'institution de l'UE à ce dernier.

24 Le résultat de l'analyse des risques liés à la protection des données pourrait également montrer que le service en nuage prévu présente des **risques liés à la protection des données qui ne peuvent pas être suffisamment maîtrisés pour réduire leur incidence de manière appropriée**. Dans ce cas, l'institution de l'UE devrait **envisager de recourir à d'autres services en nuage entraînant des risques qui peuvent être maîtrisés** de manière adéquate, voire **abandonner complètement l'«option en nuage»**.

25 Le **processus** global recommandé pour la passation de marchés publics pour des services informatiques en nuage est décrit en détail au chapitre 4.

4. Comment évaluer l'option de l'informatique en nuage, acquérir des services en nuage et les exploiter

4.1. Évaluer le caractère approprié d'un service en nuage au regard de la protection des données

26 L'acquisition de services informatiques en nuage pour traiter des données à caractère personnel peut quelque peu différer selon que:

- (Scénario I) l'institution de l'UE souhaite acquérir des services en nuage pour prendre en charge des **processus *spécifiques*** (par exemple pour gérer l'organisation des réunions de groupes d'experts), ou
- (Scénario II) le portefeuille de processus éventuels devant être pris en charge est relativement vaste et **plusieurs modèles de services** et de déploiement sont nécessaires.

Bien qu'ils partagent des caractéristiques communes, les deux scénarios sont décrits séparément.

Évaluation des risques liés à la protection des données de l'option de services en nuage

27 L'institution de l'UE doit évaluer si les **exigences en matière de conformité** avec la proposition de règlement peuvent être satisfaites.

28 L'institution de l'UE doit également réaliser une évaluation des risques liés à la protection des données à l'égard des libertés et droits fondamentaux des personnes en tenant compte des informations à sa disposition à cette étape:

- la **nature des données à caractère personnel** à traiter.

  Les données à caractère personnel qui sont, par nature, particulièrement sensibles au regard des libertés et des droits fondamentaux[20] méritent une protection spécifique;

- le **type d'opérations** à réaliser.

  Par exemple, le «profilage» est un type d'opération comportant des risques élevés possibles pour les personnes[21].

- la **portée** des opérations de traitement et leur **contexte**.

---

[20] Il s'agit en particulier des données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'adhésion à un syndicat, et le traitement des données génétiques, des données biométriques afin d'identifier de façon unique une personne physique, les données concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique ou les données liées aux condamnations et aux infractions pénales. Toutefois, il ne s'agit pas du seul facteur pour déterminer le niveau de risque. Les données à caractère personnel qui ne relèvent pas des catégories citées pourraient entraîner des niveaux de risque élevés pour les libertés et droits des personnes physiques dans certaines circonstances, notamment lorsque l'opération de traitement comprend la notation ou l'évaluation de personnes et a une incidence sur leur vie, par exemple dans un contexte financier ou professionnel, dans les processus de prise de décision automatisés avec des effets juridiques, ou du suivi systématique [par exemple par un système de télévision en circuit fermé (CCTV)]. (Voir également les «*Lignes directrices concernant l'analyse d'impact relative à la protection des données et la manière de déterminer si le traitement est "susceptible d'engendrer un risque élevé" aux fins du règlement (UE) 2016/679*» du groupe de travail «Article 29», WP 248 rév. 01http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236).

[21]Voir également les *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)* (Lignes directrices sur les décisions individuelles automatisées et sur le profilage aux fins du règlement (UE) 2016/679): http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

Réaliser des opérations sur les données concernant un grand nombre de personnes est un facteur qui peut accroître les risques.

Le contexte des opérations de traitement renvoie à la catégorie des personnes concernées (du personnel de l'UE ou non, le lieu de travail, le rôle et les tâches des personnes, la participation d'enfants, par exemple), l'incidence éventuelle de l'environnement (le préjudice éventuel causé à des personnes en raison de leur culture spécifique, par exemple), etc.;

- la **finalité** des traitements.

  Parmi les exemples: gérer des communications par courrier électronique, évaluer la performance des membres du personnel, stocker et traiter des illustrations et des vidéos des séquences de vidéosurveillance, etc.

29 Dans son évaluation, l'institution de l'UE tient compte:

- des **risques génériques liés à l'informatique en nuage** (conformément à la description de l'Annexe 4) et des **risques liés à l'option de service spécifique en nuage** et aux données à caractère personnel spécifiques ainsi qu'aux opérations de traitement relevant du champ d'application du marché public;
- de la **réalité actuelle du marché** et de la **maturité des futurs fournisseurs de services en nuage** concernant leur capacité à répondre aux exigences de conformité avec la proposition de règlement et à réduire les risques pour atteindre une ampleur acceptable. Cela peut être fait en obtenant des informations préliminaires (accessibles au public ou sur demande), y compris sur des moyens d'assurance possibles tels que ceux mentionnés à la section 4.2.1.

30 Le RGPD détermine les conditions dans lesquelles l'évaluation des risques pour les personnes est obligatoire ainsi que le contenu minimal de cette évaluation, laquelle est appelée **analyse d'impact relative à la protection des données**[22]. Le groupe de travail «Article 29» a fourni des orientations sur les conditions, les modalités et le contenu de l'analyse d'impact relative à la protection des données[23].

31 Les présentes lignes directrices ne donnent aucune indication supplémentaire sur la manière de réaliser une analyse d'impact relative à la protection des données. Le CEPD élabore actuellement des orientations pertinentes à l'intention des institutions de l'UE auxquelles il peut être fait référence à cet égard. Le DPD de l'institution de l'UE jouera un rôle essentiel en conseillant cette dernière sur le caractère obligatoire ou non de l'analyse d'impact relative à la protection des données ainsi que sur la manière de la réaliser.

32 Si une analyse d'impact relative à la protection des données est nécessaire, comme précisé dans les orientations à venir du CEPD, alors ses résultats doivent également être pris en considération au regard de l'utilisation possible du service informatique en nuage par l'institution de l'UE. Si une analyse d'impact relative à la protection des données n'est **pas** nécessaire, il peut toutefois être utile pour l'institution de l'UE d'utiliser la méthodologie pertinente de cette analyse pour réaliser l'évaluation des risques liés à la protection des données.

---

[22] Voir l'article 35 du RGPD.

[23] Disponible à l'adresse suivante: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

33 Des mesures possibles visant à respecter la proposition de règlement et à atténuer ces risques font partie des présentes lignes directrices et sont décrites aux sections 4.2, 4.3 et 4.4. Ces obligations et recommandations peuvent être considérées comme **des garanties de départ devant être mises en œuvre pour tous les services informatiques en nuage.**

34 L'existence d'une référence n'exclut pas l'obligation:

- d'évaluer les risques résiduels et les risques liés aux opérations et au contexte spécifiques que le service en nuage est censé prendre en charge (voir également Annexe 4);
- et de recenser finalement les mesures nécessaires possibles pour faire face à ces risques.

Par conséquent, une **gestion des risques documentée** par l'institution de l'UE est obligatoire dans tous les cas[24]**.**

35 Si, sur la base d'une évaluation des risques, une institution de l'UE décide de ne pas mettre en œuvre les mesures proposées en guise de référence dans le présent document, elle doit le faire d'une manière responsable et donc exposer les motifs qui justifient ce choix.

36 L'institution de l'UE doit, en tout état de cause, mettre en œuvre les mesures nécessaires conformément aux obligations prévues dans la proposition de règlement.

L'institution de l'UE évaluera enfin si les risques détectés peuvent être maîtrisés de façon à réduire de manière appropriée leur incidence et à se conformer au règlement, et décidera **si un service en nuage constitue une option adaptée ou non**.

Scénario I: passation de marchés publics pour les services d'informatique en nuage dans le cadre d'opérations spécifiques de traitement de données à caractère personnel

37 Si la conclusion de l'évaluation indique que l'institution de l'UE est, en principe, capable d'adopter des garanties visant à atténuer les risques liés à l'informatique en nuage pour l'opération de traitement spécifique ou de maîtriser de manière appropriée les risques et que, par conséquent, une décision positive est prise, les exigences en matière de protection des données (qui incluent celles en matière de sécurité) recensées lors de l'analyse des risques doivent être converties en critères dans le cahier des charges du marché public.

38 Si les exigences **ne peuvent** être satisfaites par les services en nuage disponibles, le traitement ne doit **pas** être effectué dans l'environnement de service en nuage ciblé (**décision négative**).

39 Dans ce cas, il est possible de modifier les exigences en limitant les opérations de traitement devant être prises en charge par des services en nuage aux moins risquées ou, si cela est applicable et toujours utile, en limitant les données traitées aux catégories les moins sensibles ou aux données à caractère non personnel. Une autre solution serait d'évaluer un autre modèle de déploiement/service qui comporterait des risques moins élevés. Si

[24] Voir l'article 24, paragraphe 1, du RGPD: «Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement. Ces mesures sont réexaminées et actualisées si nécessaire.»

l'institution de l'UE prévoit toujours de traiter des données à caractère personnel, elle doit réaliser une nouvelle analyse des exigences et des risques.

Scénario II: passation de marchés publics pour des contrats-cadres de services d'informatique en nuage destinés à traiter des données à caractère personnel dans un grand nombre de cas d'utilisation

40 Un processus de passation de marchés publics pour des contrats-cadres de services en nuage destinés à traiter des données à caractère personnel dans un grand nombre de cas d'utilisation (par exemple l'ensemble de l'infrastructure de TI des institutions de l'UE, les ressources de TI permettant de développer et d'exploiter les sites web institutionnels, les environnements de TI pour les développeurs, etc.), ciblant souvent les services IaaS et PaaS, pourrait prendre en considération les exigences en matière de protection des données tout au long des trois principales phases suivantes.

Phase 1: groupes de services pour un contrat-cadre

41 L'évaluation décrite ci-dessus doit être réalisée sur **un groupe d'applications/opérations de traitement candidates** pour lesquelles les services en nuage qui sont l'objet du contrat-cadre peuvent être utilisés.

42 Les exigences en matière de respect de la protection des données et les garanties déterminées au cours de l'évaluation des risques doivent être **converties en critères** dans le cahier des charges du marché public.

43 Les institutions de l'UE évalueront quelles offres de services en nuage sont adéquates et sélectionneront uniquement les fournisseurs de services capables de satisfaire ces exigences. Si aucune offre adéquate n'existe, aucun contrat ne peut être attribué.

Phase 2: caractère approprié d'une opération de traitement spécifique pour des services en nuage

44 Une fois qu'un contrat-cadre existe, il est possible que l'institution de l'UE souhaite examiner si une opération/application spécifique peut être prise en charge par l'un des services en nuage offerts par le(s) contractant(s) ayant remporté l'appel d'offres.

45 Pour une application spécifique devant être utilisée sous la forme d'un service en nuage:

L'institution de l'UE devrait **évaluer si l'un des services en nuage disponible au titre d'un contrat-cadre** est **compatible** avec les exigences en matière de protection des données de l'opération de traitement spécifique qu'il est censé prendre en charge.

46 Si les exigences **ne peuvent** être satisfaites par les services en nuage disponibles, le traitement ne doit **pas** être effectué dans l'environnement de service en nuage ciblé (**décision négative**).

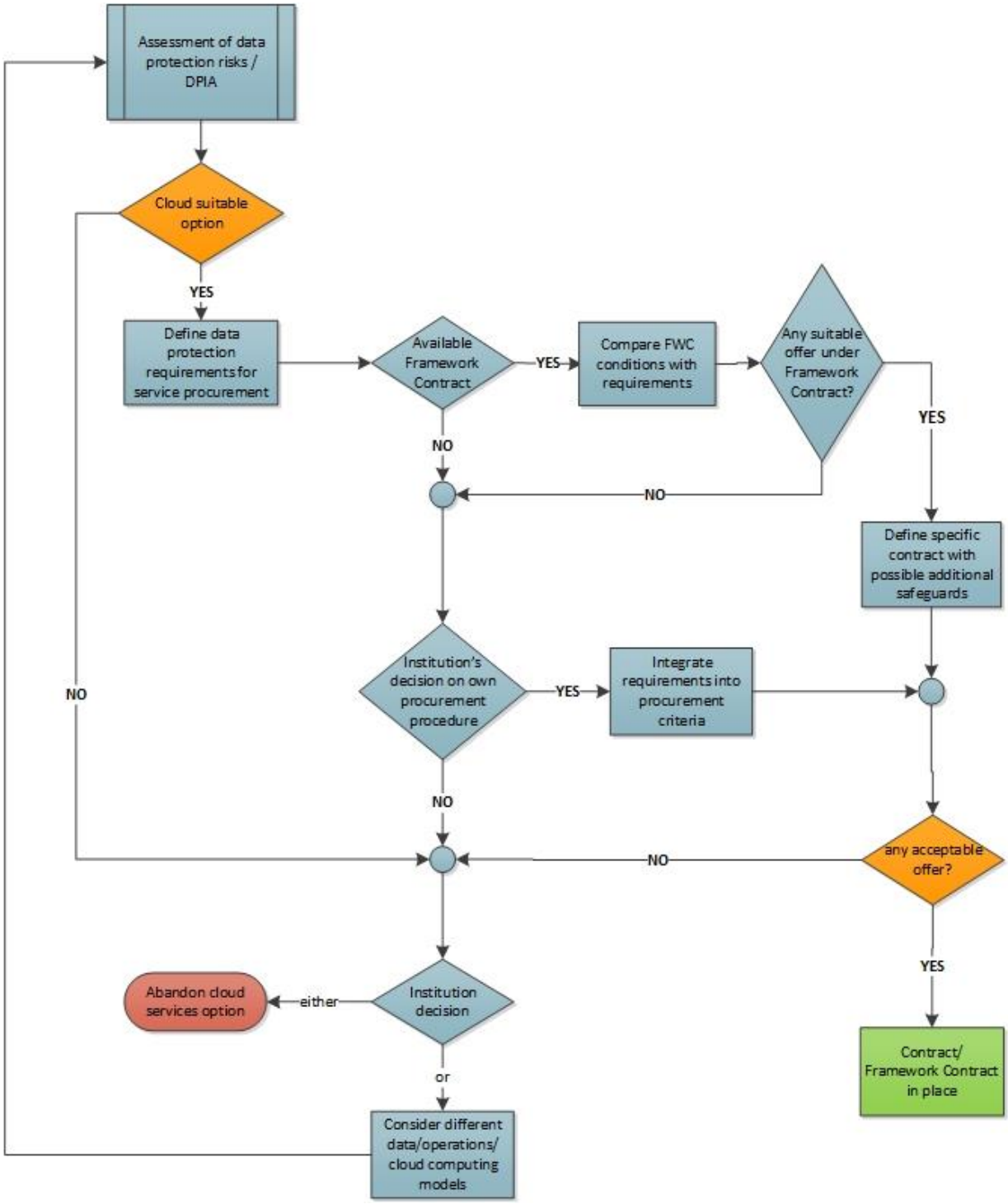
47 Dans ce cas, il est possible de modifier les exigences en limitant les opérations de traitement devant être prises en charge par des services en nuage aux moins risquées ou, si cela est applicable et toujours utile, en limitant les données traitées aux catégories les moins sensibles ou aux données à caractère non personnel. Une autre solution serait d'évaluer un autre modèle de déploiement/service qui comporterait des risques moins élevés. Si l'institution de l'UE prévoit toujours de traiter des données à caractère personnel, elle doit réaliser une nouvelle analyse des exigences et des risques.

Phase 3: passation de contrats pour des opérations de traitement spécifiques

48 Si le résultat de la phase 2 indique qu'une ou plusieurs opérations de traitement sont en principe adaptées aux services en nuage disponibles, l'institution de l'UE peut être tenue de négocier, dans les limites légalement autorisées, de nouvelles exigences possibles dans un contrat spécifique qui devra être signé afin de veiller à ce que toutes les garanties et les mesures nécessaires soient mises en place.

49 En tout état de cause, étant donné qu'une intégration renforcée peut ne pas être possible en raison des contraintes liées au marché public, il est essentiel que l'institution de l'UE tienne compte de l'ensemble des utilisations envisagées des services prévus depuis l'évaluation initiale de la phase 1 et qu'elle les définisse aussi précisément que possible.

Le processus global peut être résumé par l'organigramme suivant:



Assessment of data protection risks / DPIA	Évaluation des risques liés à la protection des données/analyse d'impact relative à la protection des données
Cloud suitable option	Option en nuage adaptée
Define data protection requirements for service procurement	Définition des exigences en matière de protection des données pour l'acquisition des services
Available Framework Contract	Contrat-cadre disponible
Compare FWC conditions with requirements	Comparaison des conditions du contrat-cadre avec les exigences

Any suitable offer under Framework Contract?	Existe-t-il une offre adéquate dans le contrat-cadre?
Define specific contract with possible additional safeguards	Définir un contrat spécifique doté de garanties supplémentaires
Institution's decision on own procurement procedure	Décision de l'institution concernant sa propre procédure de passation de marchés
Integrate requirements into procurement criteria	Intégration des exigences dans les critères du cahier des charges
any acceptable offer?	Existe-t-il une offre acceptable?
Abandon cloud service option	Abandonner l'option de service en nuage
Institution decision	Décision de l'institution
Consider different data/operations/cloud computing models	Envisager différents modèles de données/d'opération/d'informatique en nuage
Contract/Framework Contract in place	Contrat/contrat-cadre en vigueur
YES	OUI
NO	NON
either	soit
or	soit

4.2. Critères et exigences en matière d'acquisition de services en nuage

50 Une fois l'option des services en nuage choisie, les **critères et exigences** doivent être fixés pour le marché public et la gestion des services qui en résulte (exécution, maintenance, résiliation).

51 Comme pour **la procédure d'appel d'offres en général**, nous recommandons fortement aux institutions de l'UE de prendre des mesures visant à établir une **stratégie commune**[25] à l'égard de l'informatique en nuage. Cela devrait inclure la **planification** de l'acquisition des services en nuage, notamment pour accroître leur pouvoir de négociation à l'égard des fournisseurs de services en nuage, et d'autres éléments communs tels que, par exemple, un cadre pour les accords de niveau de service qui inclut des exigences en matière de protection des données, y compris notamment la gestion des contrats et le courtage[26].

[25] Voir l'avis du contrôleur européen de la protection des données relatif à la communication de la Commission intitulée «Exploiter le potentiel de l'informatique en nuage en Europe», à la page 27: «118. [...] en outre, dans le contexte du partenariat européen en faveur de l'informatique en nuage, la Commission travaillera à l'élaboration de clauses relatives à la passation de marchés spécifiques au secteur public en définissant des **exigences communes en matière de passation de marchés pour les organismes publics utilisateurs de services d'informatique en nuage**. Le CEPD souligne que ces exigences communes en matière de passation de marchés **devraient inclure** des exigences relatives à la protection des données (y compris des mesures de sécurité appropriées), lesquelles devraient être définies en fonction des risques spécifiques liés au traitement de données du secteur public dans un environnement d'informatique en nuage, sur la base d'une **analyse d'impact minutieuse relative à la protection des données**, en fonction du type et du degré de sensibilité du traitement réalisé (par exemple, en différenciant les traitements, par le secteur public, de données concernant la santé, les délits pénaux, les données confidentielles, etc.). Ainsi, les exigences contenues dans les clauses relatives à la passation de marchés devront être distinguées en fonction du degré de sensibilité des données traitées, ce qui devrait conduire à la définition de plusieurs ensembles d'exigences communes.» À cet égard, voir également la résolution du Parlement européen du 12 mars 2014.

[26] Réalisé par la Commission européenne pour le compte d'autres institutions de l'UE dans le contexte du contrat-cadre interinstitutionnel Cloud I. Une approche similaire est utilisée par les agences de l'UE dans le contexte d'un contrat-cadre géré par l'Autorité européenne de sécurité des aliments (EFSA).

52 Cela pourrait résoudre en partie les difficultés potentielles des petites institutions de l'UE qui disposent de leurs propres procédures d'appels d'offres lorsqu'il s'agit de définir les exigences contractuelles et d'intégrer des garanties spécifiques dans le contrat-cade/le cahier des charges.

4.2.1. Diligence dans le choix d'un candidat fournisseur de services en nuage

53 L'institution de l'UE doit choisir un fournisseur de services en nuage **qui donne l'assurance suffisante d'agir au nom de l'institution de l'UE et de mettre en œuvre les mesures techniques et organisationnelles nécessaires en matière de protection des données**, et doit vérifier l'efficacité de ces mesures.

54 Les éléments probants sur lesquels une institution de l'UE peut s'appuyer pour contribuer à cette assurance sont entre autres:

- **des certifications de protection des données et de sécurité des TI octroyées par des tiers** dans le cadre de programmes de certification pertinents[27]. Celles-ci doivent inclure les programmes de certification de sécurité des TI et de protection des données liées au nuage qui répondent aux risques recensés[28]. En général, les auto-évaluations ne doivent pas être considérées comme apportant un degré suffisant d'assurance;
- l'application de **codes de conduite spécifiques au nuage** qui fournissent une valeur ajoutée en termes de mesures destinées à protéger les données à caractère personnel et contribuent à démontrer la conformité avec le règlement dans un environnement spécifique au nuage[29];
- **une expérience précédente concernant des projets** présentant des risques similaires (ou plus élevés) pour des catégories analogues de données à caractère personnel. Une assurance supplémentaire peut être fournie par une expérience avérée auprès des administrations publiques nationales ou de l'UE;
- **les pratiques en matière de responsabilité déjà en place** comme: un délégué à la protection des données au sein de l'entreprise; des procédures et des politiques en matière de vie privée en place; la participation à des analyses d'impact relatives à la protection des données ou en tous cas l'existence d'une méthodologie permettant d'évaluer les risques liés à la protection des données; l'utilisation de clauses contractuelles types[30] (le cas échéant); l'utilisation de règles d'entreprise contraignantes (le cas échéant); un cadre de gestion des risques des TI en place; des politiques, des procédures et des garanties en matière de sécurité des TI déjà en place.

---

[27] Le groupe de travail «Article 29» fournit des orientations sur l'établissement de **programmes de certification** susceptibles de contribuer à démontrer la conformité au titre des dispositions du RGPD. Une liste de ces programmes sera mise à disposition par les autorités nationales chargées de la protection des données ou par le futur comité européen de la protection des données.

[28] L'article 28, paragraphe 5, du RGPD établit que les sous-traitants (dans le cas présent, les fournisseurs d'accès en nuage) peuvent s'appuyer sur les **mécanismes de certification** (visés à l'article 42 du RGPD) en tant qu'élément pouvant garantir la mise en œuvre de mesures techniques et organisationnelles appropriées.

[29] Le groupe de travail «Article 29» fournira des orientations sur les **codes de conduite** susceptibles de contribuer à démontrer la conformité au titre des dispositions du RGPD. Une liste de ces codes de conduite sera mise à disposition par les autorités nationales chargées de la protection des données ou par le futur comité européen de la protection des données.

[30] Il est fait référence en particulier aux clauses contractuelles types aux paragraphes 6 à 8 de l'article 29 du RGPD.

4.2.2. Passation de contrats: définir les bonnes conditions pour le futur fournisseur de services en nuage[31]

(i) Introduction et remarques générales

55 Pour veiller à ce que l'institution de l'UE garde le contrôle sur la manière dont le fournisseur de services en nuage fournit les services demandés, il est essentiel de **négocier et d'obtenir des conditions appropriées dans le contrat conclu avec le fournisseur de services en nuage.** Certaines de ces conditions sont précisées ci-dessous (en tant que «clauses types»).

56 Il importe de souligner que ces conditions doivent être **adaptées** afin de tenir compte des contraintes juridiques applicables aux institutions de l'UE (en particulier, de l'applicabilité du protocole sur les privilèges et immunités de l'Union européenne[32]) et **ajustés** selon la nécessité de répondre aux risques posés par le traitement des données (selon une approche «fondée sur le risque).

(ii) Évaluation générale des modalités contractuelles

57 Les responsables du traitement doivent être conscients de l'importance de **l'évaluation générale du cadre contractuel** applicable à la fourniture des services en nuage[33].

- Cela signifie que l'institution de l'UE devrait évaluer **l'ensemble des éléments** (y compris par exemple les annexes) des documents contractuels du fournisseur de services en nuage qui décrivent spécifiquement l'opération de traitement couverte par

---

[31] Concernant cette question de manière générale, il convient de consulter l'avis du contrôleur européen de la protection des données relatif à la communication de la Commission intitulée «Exploiter le potentiel de l'informatique en nuage en Europe», aux pages 26 et 27, paragraphe 117.

[32] Voir la note de bas de page 17.

[33] Pour une **liste de contrôle rapide**, voir l'avis 05/2012 du groupe de travail «Article 29» sur l'informatique en nuage, section 3.4.2 **«Garanties contractuelles de la ou des relation(s) responsable du traitement/sous-traitant»**, pages 12 à 14 établissant 14 points, parmi lesquels nous attirons l'attention sur:

Point 5 – «L'inclusion d'une **clause de confidentialité** liant le fournisseur d'informatique en nuage à l'un quelconque de ses employés qui peut avoir accès aux données. Seules les personnes autorisées peuvent avoir accès aux données.»

Point 7 – «Le contrat devrait expressément établir que **le fournisseur d'informatique en nuage ne peut pas communiquer les données à des tiers**, même à des fins de conservation, sauf si le contrat prévoit le recours à des sous-traitants. Le contrat devrait préciser que les sous-traitants ultérieurs ne peuvent être mandatés que sur la base d'une autorisation généralement donnée par le responsable du traitement, qui s'accompagne de l'obligation claire pour le sous-traitant d'informer le responsable du traitement de toute proposition de modification à cet égard, celui-ci conservant à tout moment la possibilité de contester ces modifications ou de résilier le contrat. Le fournisseur d'informatique en nuage doit être clairement tenu de **donner le nom de tous les sous-traitants mandatés** (par exemple, sur un registre public numérique). Il faut s'assurer que le contrat signé entre le fournisseur d'informatique en nuage et le sous-traitant reflète les dispositions du contrat signé entre le fournisseur d'informatique en nuage et son client (à savoir que les sous-traitants ultérieurs sont soumis aux mêmes obligations contractuelles que les fournisseurs d'informatique en nuage). En particulier, il doit être garanti que le fournisseur d'informatique en nuage et tous les sous-traitants n'agissent que sur instruction du client. (…) la **chaîne de responsabilité** devrait être clairement établie dans le contrat, tout comme l'obligation du sous-traitant d'encadrer les transferts internationaux, par exemple en signant des contrats avec les sous-traitants ultérieurs, sur la base des clauses contractuelles types issues de la décision de la Commission européenne du 5 février 2010 (2010/87/UE).»

Point 11 – «Il convient d'établir contractuellement que le fournisseur d'informatique en nuage est tenu d'**informer son client** des changements pertinents relatifs aux différents services en nuage, comme la mise en œuvre de fonctions supplémentaires, par exemple.»

Point 12 – «Le contrat devrait prévoir la **journalisation et l'audit** des opérations de traitement des données à caractère personnel effectuées par les employés du fournisseur d'informatique en nuage ou par les sous-traitants.»

l'accord (par exemple les catégories de données traitées, les mesures de sécurité et de confidentialité mises en œuvre par le fournisseur de services en nuage, etc.). L'institution de l'UE doit évaluer **au cas par cas** la manière dont le contrat, l'accord de niveau de service et leurs annexes (c'est-à-dire, le cadre contractuel global) répondent aux besoins spécifiques et aux exigences légales en matière de protection des données.

- Il est particulièrement essentiel de vérifier les «**autres** clauses contractuelles» (c'est-à-dire les clauses qui ne sont **pas directement liées à la protection des données, mais qui sont toutefois importantes pour garantir la responsabilité**), y compris les clauses relatives à la **législation applicable au contrat en lui-même** («droit applicable») et à la **juridiction compétente**; au **droit des parties d'apporter des modifications au contrat**; aux **obligations du fournisseur de services en nuage après la résiliation du service de traitement des données «externalisées» par l'institution de l'UE**.

58 Il convient d'établir également dans le contrat concernant les services en nuage les clauses relatives à la **disponibilité et à la qualité du service** (établir les délais dans lesquels le service doit être disponible ainsi que les caractéristiques techniques, l'efficacité et l'efficience, et définir des indicateurs pertinents). Ces dispositions sont très souvent regroupées dans un accord de niveau de service.

59 En règle générale, il convient de rappeler que les fournisseurs de services en nuage offrant des services à des clients soumis à des législations de l'UE ont l'obligation d'évaluer la conformité de leurs modalités contractuelles avec les exigences de l'UE en matière de protection des données sur la base de la proposition de règlement, en tenant compte des défis posés par l'informatique en nuage pour la protection des données, conformément à la description faite dans l'avis 05/2012 du groupe de travail «Article 29» sur l'informatique en nuage ainsi que dans l'avis pertinent du CEPD[34].

(iii) Concernant certaines questions «essentielles» de protection de données auxquelles les conditions contractuelles doivent répondre

60 Il est essentiel d'ajouter aux modalités du contrat qu'il est **interdit** pour les fournisseurs de services en nuage **de divulguer** aux **autorités répressives** des États membres de l'UE ou des pays tiers les données à caractère personnel qui leur sont confiées par l'institution de l'UE, *sauf autorisation expresse prévue par la législation de l'UE, ou par la législation d'un État membre dans la mesure où les conditions établies dans la législation de l'UE concernant la divulgation sont remplies*[35].

61 La **transparence** est un élément important de la relation entre l'institution de l'UE et le fournisseur de services en nuage, car **elle a une incidence directe sur le respect des**

[34] Voir la note de bas de page 10.

[35] Cette interdiction est une obligation légale découlant du **protocole sur les privilèges et immunités de l'Union européenne**. Toutefois, il serait utile de rappeler ce principe à l'intention du fournisseur de services en nuage dans les conditions du contrat de service. Conformément à l'article 1er du protocole susmentionné: [...] «*les biens et avoirs des Communautés ne peuvent être l'objet d'aucune mesure de contrainte administrative ou judiciaire sans une autorisation de la Cour de justice*». En ce qui concerne cette disposition, nous observons qu'elle pourrait également couvrir les services d'informatique en nuage pour lesquels une licence d'utilisation a été octroyée aux organes et institutions de l'UE. L'article 2 dispose que: «*Les archives des Communautés sont inviolables*». L'article 6 dispose ce qui suit: «*Pour leurs communications officielles et le transfert de tous leurs documents, les institutions des Communautés bénéficient, sur le territoire de chaque État membre, du traitement accordé par cet État aux missions diplomatiques.*»

obligations de l'institution de l'UE au titre de la proposition de règlement. Par conséquent, toute modification pertinente apportée à l'infrastructure, aux procédures et aux résultats sous-jacents des audits de sécurité dans ce domaine devrait être **communiquée** par le fournisseur de services en nuage à l'institution de l'UE en temps voulu, sous garantie de la confidentialité. Cela peut également inclure des informations concernant l'activation de mesures de continuité des activités, des tests ou toute opération ayant une incidence potentielle sur le service au consommateur.

62 Étant donné que l'institution de l'UE est responsable de la licéité du traitement des données, elle a le droit de demander au fournisseur de services en nuage de l'**informer immédiatement** si celui-ci ne peut garantir la conformité avec les obligations prévues dans le contrat. En ce qui concerne la transparence, il est important de mentionner (dans l'accord de niveau de service ou dans le contrat) **l'ensemble des sous-traitants ultérieurs** qui contribuent à fournir le service en nuage, ainsi que les **lieux où** les données à caractère personnel peuvent être traitées.

63 La **localisation** de l'entreprise fournissant le service en nuage, de ses centres de données hébergeant les serveurs et d'autres équipements dans lesquels les données sont stockées ou traitées (y compris à des fins de sauvegarde, de continuité des activités et de transit, ainsi que les lieux depuis lesquels des opérations éloignées sont réalisées) est également un facteur essentiel à prendre en considération.

- À **cet égard, le CEPD recommande que le traitement des données à caractère personnel confié par des institutions de l'UE à des fournisseurs de services en nuage, et à des sous-traitants, ait lieu, *en règle générale*, au sein de l'UE**[36].

  L'objectif de cette recommandation est de garantir l'applicabilité (notamment dans l'«environnement en nuage») des privilèges et immunités dont jouissent les institutions de l'UE sur le territoire de ses États membres conformément au **protocole sur les privilèges et immunités de l'Union européenne**[37]**.**

  D'après l'article 1er du protocole, «[l]es locaux et les bâtiments de l'Union sont inviolables. Ils sont exempts de perquisition, réquisition, confiscation ou expropriation. Les biens et avoirs de l'Union ne peuvent faire l'objet d'aucune mesure de contrainte administrative ou judiciaire sans une autorisation de la Cour de justice». L'article 2 dispose que «[l]es archives de l'Union sont inviolables». Enfin, selon l'article 5, «[p]our leurs communications officielles et le transfert de tous leurs documents, les institutions de l'Union bénéficient sur le territoire de chaque État membre du traitement accordé par cet État aux missions diplomatiques».

  Outre ces éléments, nous tenons compte du fait que, lorsque les données sont stockées sur le territoire d'un pays tiers, les autorités répressives locales compétentes du territoire peuvent solliciter l'accès aux données dans le contexte d'une mesure

---

[36] Par exemple, l'EFSA a veillé à introduire la clause suivante dans le contrat de service d'informatique en nuage devant être passé par l'agence de l'UE: *«Les services d'informatique en nuage sont hébergés uniquement sur le territoire de l'Espace économique européen. Le fournisseur de services en nuage, ses affiliés et ses sous-traitants ultérieurs hébergeront les données (de l'agence de l'UE), y compris les données de sauvegarde, sur des supports de stockages et dans des centres de données situés dans **les États membres de l'UE suivants***».

[37] Concernant les protections reconnues par les États membres de l'UE aux institutions de l'UE conformément au protocole, voir, en particulier, les articles 1er, 2 et 5 du protocole, disponible, dans sa version consolidée, à l'adresse suivante: http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:12012E/PRO/07&from=FR.

d'**application de leur législation publique** (par exemple législations pénale, procédurale ou en matière de rétention de données, etc.). L'institution de l'UE doit analyser ce risque avec attention.

Il convient également de noter que, si la localisation de l'hébergement de l'infrastructure en nuage est située dans un **pays tiers**, il sera **plus difficile pour le CEPD de coopérer et de coordonner les inspections** avec les autorités de contrôle compétentes et donc de garantir l'application globale des règles du règlement[38].

(iv) Clauses types (éléments à vérifier, aspects à définir/inclure dans le contrat)

64 Une partie du contenu de la présente section pourrait également prendre la forme d'un accord de niveau de service (voir section 4.3.2), comme les dispositions en matière de sécurité. L'accord de niveau de service devrait faire partie de l'accord contractuel contraignant (il appartient toutefois à l'institution de l'UE de décider de la manière d'organiser les dispositions contractuelles et de répartir les conditions dans le contrat et/ou dans l'accord de niveau de service).

65 Sur la base des clauses contractuelles les plus pertinentes et les plus fréquemment utilisées[39], nous fournissons des clauses types à inclure dans le contrat. Ces **clauses types** sont établies

---

[38] Nous soulignons que le RGPD prévoit une obligation de **coopération entre les autorités de contrôle nationales** au titre du chapitre VII.

Il convient également de noter que, en application de l'article 58, paragraphe 1, point f), du RGPD, les autorités de contrôle disposent du pouvoir d'enquêter afin d'«obtenir l'accès à tous les locaux du responsable du traitement **et du sous-traitant**, notamment à toute installation et à tout moyen de traitement, **conformément au droit de l'Union ou au droit procédural des États membres**» (*caractère gras ajouté).*

Nous soulignons que, *si* des données à caractère personnel sont traitées **en dehors de l'UE**, les dispositions suivantes du RGPD s'appliquent (c'est-à-dire le chapitre V, articles 44 à 50).

Pour les orientations du CEPD, sur la base des dispositions du règlement (CE) nº 45/2001 actuel, voir le document d'orientation du CEPD «Orientations sur les transferts à des pays tiers et à des organisations internationales: article 9», disponible à l'adresse:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_FR.pdf. Ce document sera mis à jour à la lumière des dispositions de la proposition de règlement.

[39] Notamment les clauses contenues dans la décision C(2010)593 de la Commission, disponible à l'adresse:

http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_fr.htm.

Il convient de noter que la possibilité pour le responsable du traitement d'avoir recours à des clauses types de protection de données ne devrait ni empêcher le fournisseur de services en nuage d'inclure les clauses types de protection des données dans un contrat plus large ni l'empêcher d'ajouter d'autres clauses pour autant qu'elles ne soient pas en contradiction, directement ou indirectement, avec les clauses contractuelles types adoptées par la Commission ou par les autorités de contrôle et sans préjudice des libertés et des droits fondamentaux des personnes concernées.

Il conviendrait également de tenir compte de la mise à jour récente (29 novembre 2017) du «Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes» (WP 256) (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109) et du «Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes applicables aux sous-traitants» (WP 257) (http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110). Ces documents établissent un tableau présentant les éléments et principes que doivent contenir les règles d'entreprise contraignantes en vue de refléter les exigences relatives à ces règles expressément prévues dans le RGPD (article 47). Une disposition comparable à l'article 47, paragraphe 2, du RGPD, décrivant le contenu des clauses contractuelles types, n'est pas

pour **aider l'institution de l'UE à contrôler rapidement si le contrat relatif à la fourniture des services en nuage offre des garanties adéquates en matière de protection des données.** Ces clauses doivent être **adaptées** au service en nuage spécifique offert (par exemple, en tenant compte du fait que le fournisseur de services en nuage a recours ou non à des sous-traitants ultérieurs).

66 Les clauses types sont les suivantes:

A - Description du traitement pris en charge

La description du traitement et, en particulier, des catégories de données à caractère personnel qui font l'objet d'un traitement par le fournisseur de services en nuage est donnée, selon le cas, dans ce contrat et dans l'accord de niveau de service et ses annexes, qui font partie intégrante du contrat[40].

B - Droit applicable en matière de protection des données

67 Le traitement des données à caractère personnel doit être réalisé conformément aux dispositions pertinentes de [la proposition de règlement] et fournir, entre autres, aux personnes concernées des droits spécifiques (au titre du chapitre III, articles 14 à 25) et conformément aux dispositions du contrat, de l'accord de niveau de service et de ses annexes.

68 Toute modification de la législation applicable au fournisseur de services en nuage, l'empêchant de suivre les instructions reçues de l'institution de l'UE et de respecter les obligations prévues dans le contrat et susceptible d'avoir des conséquences négatives importantes sur les garanties et les obligations prévues par les clauses, doit être rapidement notifiée par le fournisseur de services en nuage à l'institution de l'UE dès que celui-ci a connaissance de cette modification législative, même avant l'entrée en vigueur de celle-ci. Dans ce cas, l'institution de l'UE a le droit de suspendre et/ou de résilier le contrat.

69 Le fournisseur de services en nuage est tenu de fournir à l'institution de l'UE des **informations exhaustives sur la localisation physique** des serveurs utilisées par ledit fournisseur et ses sous-traitants ultérieurs pour les services en nuage fournis (y compris à des fins de sauvegarde, de continuité des activités et de transit) ainsi que les emplacements à partir desquels les opérations à distance sont réalisées. Tout projet de modification de la localisation doit être soumis par le fournisseur de services en nuage à l'institution de l'UE préalablement au traitement des données au nouvel emplacement et doit être précédé d'un préavis nécessaire pour que l'institution de l'UE puisse vérifier en particulier si le

établie au titre du RGPD. Toutefois, il est vrai que certaines garanties au titre de l'article 47, paragraphe 2, peuvent également s'appliquer aux clauses types de protection des données visées à l'article 46 du RGPD.

[40] Conformément à l'article 28, paragraphe 3, et à l'article 28, paragraphe 9, du RGPD, les éléments suivants décrivant le traitement doivent dans tous les cas être définis dans le contrat, lequel se présente sous une forme écrite, y compris en format électronique: l'objet et la durée du traitement; la nature et la finalité du traitement; le type de données à caractère personnel et les catégories de personnes concernées; les droits et les obligations du responsable du traitement.

changement est conforme au contrat et à la législation applicable [41]. L'institution de l'UE a le droit de s'opposer au changement.

C - Droit contractuel applicable

70 Les clauses ou le contrat sont régis par la législation de l'UE et, le cas échéant conformément à la législation de l'UE, par la législation de l'État membre de l'UE dans lequel l'institution de l'UE est établie ou toute autre législation applicable d'un État membre de l'UE.

D - Modification du contrat

71 Le fournisseur de services en nuage et l'institution de l'UE s'engagent à ne pas modifier les clauses. Cela n'empêche pas le fournisseur de services en nuage et l'institution de l'UE d'ajouter d'autres dispositions contractuelles concernant les questions à caractère commercial en cas d'accord en ce sens et dans la mesure où ils ne s'écartent pas de la législation applicable en matière de protection des données.

E - Obligation après la résiliation des services de traitement de données à caractère personnel

72 À la résiliation des **services de traitement** de données, le fournisseur de services en nuage et ses sous-traitants ultérieurs doivent, selon le choix de l'institution de l'UE:

- sans délai, sous un format convenu en commun, soit **restituer l'ensemble des données à caractère personnel et leurs copies à l'institution de l'UE**, soit **les transférer vers une destination désignée** par l'institution de l'UE elle-même, ou
- **supprimer effectivement l'ensemble des données à caractère personnel et certifier à l'institution de l'UE que cela a été fait,** une fois qu'il a été vérifié et confirmé que les données ont été transférées complètement et avec succès au nouveau sous-traitant ou à l'institution de l'UE.

F – «Portabilité» des données transférées au fournisseur de services en nuage (en tant que droit pour l'institution de l'UE de recevoir et de transmettre ces données à un autre fournisseur de services en nuage)

73 Le fournisseur de services en nuage doit garantir et être capable de démontrer la **«portabilité» des données de l'institution de l'UE depuis ses systèmes, et depuis tout système de ses sous-traitants ultérieurs, à d'autres fournisseurs** choisis par l'institution de l'UE, dans les *[...]* heures au format précisé *[dans l'accord de niveau de service et/ou...]* après avoir reçu une notification écrite de l'institution de l'UE. Le fournisseur de services en nuage doit garantir que l'institution de l'UE obtient intégralement le service et l'accès aux données au cours de cette période.

74 Le fournisseur de services en nuage et ses sous-traitants ultérieurs doivent garder les données de l'institution de l'UE en sécurité jusqu'à ce qu'elles soient transférées vers un autre site sous le contrôle de l'institution de l'UE.

[41] Cela pourrait également être défini plus précisément conformément aux besoins de l'institution de l'UE.

G - Responsabilité unique du traitement

75 Le fournisseur de services en nuage doit traiter les données à caractère personnel **uniquement au nom de l'institution de l'UE** et **conformément avec ses clauses et instructions documentées**. S'il ne peut le faire, il doit en informer l'institution de l'UE dans les meilleurs délais. Dans ce cas, l'institution de l'UE a le droit de suspendre ou de résilier le contrat.

H - Sous-traitance

76 Le fournisseur de service en nuage garantit, surveille et contrôle que, dans le cas d'une sous-traitance, l'activité est menée par un sous-traitant ultérieur offrant au moins le même niveau de protection des données à caractère personnel et des libertés et droits fondamentaux des personnes concernées que lui-même en vertu des clauses convenues.

77 Dans le cas d'une sous-traitance, le fournisseur de services en nuage s'assure d'avoir **préalablement informé l'institution de l'UE** de ses projets; d'avoir fourni des **informations exhaustives** sur les sous-traitants ultérieurs éventuels (quant à leur capacité à fournir une assurance suffisante, conformément à la description faite à la section 4.2.1) et leur rôle futur dans le service en nuage; et d'avoir obtenu de l'institution de l'UE son **consentement écrit préalable (autorisation écrite spécifique ou générale)**. Le fournisseur **envoie** à l'institution de l'UE, dans les meilleurs délais, **un exemplaire de tout accord de sous-traitance** conclu.

78 Si le fournisseur de services en nuage sous-traite ses obligations au titre des clauses, moyennant l'approbation préalable de l'institution de l'UE **(autorisation écrite spécifique ou générale)**, il le fait uniquement au moyen d'un **accord écrit avec le sous-traitant ultérieur imposant à ce dernier les mêmes obligations que celles qui incombent au fournisseur de services en nuage en vertu des clauses.**

[Cette exigence peut être satisfaite si **le sous-traitant ultérieur annexe** les parties pertinentes du contrat-cadre conclu entre l'institution de l'UE et le fournisseur de services en nuage au contrat passé entre celui-ci et le sous-traitant ultérieur.]

Si le sous-traitant ultérieur manque à ses obligations en matière de protection des données au titre dudit accord écrit, le fournisseur demeure entièrement responsable auprès de l'institution de l'UE de l'exercice des obligations du sous-traitant ultérieur.

Les aspects de la sous-traitance liés à la protection des données sont régis par [la proposition de règlement].

I - Obligation du fournisseur de services en nuage de coopérer et d'informer l'institution de l'UE

79 Le fournisseur de services en nuage traite dans les meilleurs délais et de manière appropriée toutes les demandes de l'institution de l'UE liées au traitement des données à caractère personnel par ledit fournisseur.

80 Le fournisseur de services en nuage informe l'institution de l'UE dans les meilleurs délais de l'existence d'une législation qui s'applique à lui ou à ses sous-traitants ultérieurs et qui l'empêche de traiter les données à caractère personnel uniquement sur instruction de l'institution de l'UE ou qui empêche la réalisation d'un audit du fournisseur de services en nuage ou de ses sous-traitants ultérieurs.

81 Dans ce cas, l'institution de l'UE peut demander la suspension du traitement des données par le fournisseur de services en nuage et/ou la résiliation du contrat.

82 Le fournisseur de services en nuage informe l'institution de l'UE:

(i) des modifications futures concernant le service en nuage, telles que la mise en œuvre de fonctions supplémentaires, en temps voulu;

(ii) des modifications futures de l'infrastructure et des procédures ayant une incidence potentielle sur le service et, en temps voulu, des résultats des audits de sécurité dans ce domaine, sous garantie de la confidentialité;

(iii) des demandes juridiquement contraignantes de divulgation de données à caractère personnel provenant d'autorités répressives selon les modalités prévues dans les clauses conformément à la législation applicable;

(iv) des incidents liés à la sécurité (et fournit une assistance adéquate afin de gérer de manière appropriée les risques éventuels liés à la protection des données posés par ces incidents), selon les modalités prévues dans les clauses conformément à la législation applicable;

(v) sans délai, toute demande liée à l'exercice des droits des personnes concernées reçues directement de ces personnes. Dans ce cas, le fournisseur de services en nuage ne répond pas à ces demandes, sauf instruction contraire de l'institution de l'UE, et fournit à celle-ci les outils et informations nécessaires pour gérer les données à caractère personnel des personnes concernées, et notamment l'accès, la suppression, la rectification, le verrouillage, etc.

J - Obligation d'informer le CEPD et de coopérer avec lui

83 Le fournisseur de services en nuage est conscient que le CEPD a le droit de mener des visites, des audits et des inspections auprès dudit fournisseur[42], et de ses sous-traitants ultérieurs, dans les mêmes conditions que celles qui s'appliquent à un audit de l'institution de l'UE elle-même au titre de [la proposition de règlement]. L'audit a pour objectif de contrôler la conformité du traitement des données confié par l'institution de l'UE au fournisseur de

[42] Pour permettre tant à l'institution de l'UE qu'au CEPD de contrôler les opérations de traitement du fournisseur de services en nuage, l'article 30 du RGPD prévoit l'obligation que les fournisseurs de services en nuage (en tant que sous-traitants) «tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant:

a) le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que le nom et les coordonnées du délégué à la protection des données;

b) les catégories de traitements effectués pour le compte de chaque responsable du traitement;

c) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et les documents attestant de l'existence de garanties appropriées;

d) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 33.

3. Les registres visés aux paragraphes 1 et 2 se présentent sous une forme écrite y compris la forme électronique».

services en nuage avec les obligations contractuelles ainsi que les principes et règles applicables en matière de protection des données.

84 Le fournisseur de services en nuage coopère dûment lors de ces inspections et à titre gracieux.

K - Mesures de sécurité

85 Le fournisseur de services en nuage s'assure de **disposer d'un cadre de gestion des risques liés à la sécurité des TI adapté**[43] et d'avoir mis en œuvre les mesures techniques et de sécurité nécessaires fixées au titre du cadre pertinent ainsi que les mesures précisées dans le contrat et/ou l'accord de niveau de service avant de traiter les données pour le compte de l'institution de l'UE, et il veille à conserver ce cadre et à gérer les risques tout au long de la durée du contrat de manière adéquate.

86 Lorsqu'il évalue le niveau de sécurité approprié, le fournisseur de services en nuage tient compte en particulier des risques présentés par le traitement, notamment ceux découlant de la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

87 Le fournisseur de services en nuage conserve une documentation concernant le cadre et les mesures techniques et de sécurité en vigueur et fournit à l'institution de l'UE l'accès adéquat à celle-ci, afin de lui permettre de respecter les exigences de [la proposition de règlement].

L - Notification de violation des données

88 Le fournisseur de services en nuage met en œuvre des mécanismes appropriés pour traiter les incidents liés à la sécurité et les violations de données à caractère personnel dans les meilleurs délais et de manière efficace. Cela inclut des mécanismes de notification garantissant que l'**institution de l'UE est informée de toute violation possible de données à caractère personnel**[44] (incidents liés à la sécurité affectant les données à caractère personnel traitées pour le compte de l'institution de l'UE).

89 Le fournisseur de services en nuage notifie toutes les violations de données à caractère personnel à l'institution de l'UE sans délai et, dans la mesure du possible, en temps voulu pour que l'institution de l'UE puisse informer, si nécessaire sur la base des exigences de [la proposition de règlement], les personnes concernées touchées sans délai et le CEPD dans les 72 heures après que le fournisseur de services en nuage a pris connaissance de la violation.

90 Le fournisseur de services en nuage fournit aux institutions de l'UE à tout le moins les informations suivantes:

---

[43] Voir également les orientations du CEPD visées à la note de bas de page 51

[44] Pour davantage d'orientations sur les violations de données à caractère personnel, voir le projet d'avis actuel du groupe de travail «article 29», disponible à l'adresse suivante: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Le RGDP contient, en ses articles 33 et 34, des dispositions spécifiques sur la notification des violations de données à caractère personnel à l'autorité de contrôle et à la personne concernée.

- la nature de la violation de données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
- les conséquences probables de la violation de données à caractère personnel;
- les mesures prises ou proposées pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

91 Le fournisseur de services en nuage collabore avec les institutions de l'UE pour pouvoir se conformer à l'ensemble des obligations pertinentes établies dans la [proposition de règlement] concernant les violations de données à caractère personnel.

92 Des informations supplémentaires concernant le contenu et la forme de la notification sont définies dans l'accord de niveau de service.

M - Audit (au cours et au terme de l'activité de traitement des données)

93 Le fournisseur de services en nuage et son sous-traitant ultérieur mettent en œuvre des mécanismes en faveur de **l'enregistrement des opérations de traitement** concernant les données à caractère personnel réalisées pour le compte de l'institution de l'UE.

94 Le fournisseur de services en nuage permet la réalisation d'éventuels **audits** de ses activités de traitement par l'institution de l'UE et contribue à ces audits, sur la base des dispositions pertinentes de [la proposition de règlement][45]. L'audit peut être mené par un **tiers** choisi par l'institution de l'UE, possédant les qualifications professionnelles requises et tenu à un devoir de confidentialité.

95 Le fournisseur de services en nuage et le sous-traitant ultérieur permettent la réalisation d'audits de leurs installations de traitement de données et contribuent à ces audits, sur demande de l'institution de l'UE et/ou du CEPD, relatifs aux mesures prises par le fournisseur de services en nuage pour se conformer aux obligations qui lui incombent à la résiliation des services de traitement des données à caractère personnel.

N - Accès des autorités répressives

96 Au titre de l'article 2 du protocole sur les privilèges et immunités de l'Union européenne, «[l]es archives des Communautés sont inviolables». En tant qu'organe de l'UE, l'institution de l'UE est soumise aux privilèges et immunités de l'Union européenne, en particulier en ce qui concerne l'inviolabilité des archives (y compris la localisation physique des données et services) et la sécurité des données.

97 Le fournisseur de services en nuage notifie sans délai à l'institution de l'UE toute demande juridiquement contraignante de divulgation de données à caractère personnel traitées pour le compte de l'institution de l'UE et émanant d'une autorité publique (par exemple le

[45] Article 28, paragraphe 3, point h), du RGPD.

procureur d'un État membre), y compris de pays tiers[46]. Le fournisseur de services en nuage ne donne pas accès aux données à caractère personnel sauf sous autorisation de l'AIPN (autorité investie du pouvoir de nomination) de l'institution de l'UE concernée.

O - Niveau de service

98 Le fournisseur de services en nuage exécute le service conformément à un accord de niveau de service, lequel fait intégralement partie du contrat.

P - Voie de recours contractuelle

99 Tout écart ou infraction aux points cités ci-dessus peut constituer un motif pour que l'institution de l'UE résilie le contrat avec effet immédiat, sans préjudice de dommages éventuels.

4.3. Exploitation du service en nuage

100 Des garanties sont nécessaires au cours de l'exploitation des services en nuage afin de protéger les données à caractère personnel et de respecter les obligations et principes applicables en matière de protection des données[47].

101 Les questions déléguées au fournisseur de services en nuage agissant en tant que sous-traitant devraient être décrites dans le contrat (voir la section 4.2), dans lequel certains aspects opérationnels sont généralement définis dans un accord de niveau de service (voir la section 4.3.2) et doivent être gérés. Les éléments devant être directement exécutés par l'institution de l'UE (voir la section 4.3.1) dépendent en grande partie du modèle de déploiement et de service en nuage (voir Annexe 3 pour leur définition).

4.3.1. Tâches sous le contrôle direct de l'institution de l'UE

102 L'institution de l'UE met en place l'infrastructure organisationnelle interne nécessaire pour garantir que les services d'informatique en nuage sont exploités conformément aux règles en matière de protection des données[48].

---

[46] L'institution de l'UE fournira au destinataire de l'État membre (tel que le procureur national susmentionné) l'accès aux données uniquement si les conditions prévues dans la législation de l'UE concernant la divulgation sont remplies.

[47] L'institution de l'UE conserve l'ensemble de ses responsabilités concernant les questions de conformité en tant que responsable du traitement, même si les opérations sont menées par l'intermédiaire d'un fournisseur de services en nuage. Ces responsabilités sont notamment: la licéité, la nécessité et la proportionnalité; la définition et la limitation des finalités; la qualité des données, y compris les durées de conservation; l'information aux personnes concernées et les droits de ces personnes (accès, modification, suppression, verrouillage); les transferts possibles; les dispositions en matière de réseaux de télécommunications internes, le cas échéant; l'accès des autorités de contrôle ainsi que toutes autres dispositions applicables.

[48] À cet égard, en tant que source de bonnes pratiques et liste de contrôle, intégrant également des **programmes de formation, de contrôle et d'audit**, il convient de consulter l'avis 02/2014 du groupe de travail «Article 29» relatif à un référentiel des exigences pour les règles d'entreprise contraignantes soumises aux autorités nationales responsables de la protection des données dans l'UE et les règles transfrontalières de protection de la vie privée soumises aux agents de responsabilisation de l'APEC en matière de RTPVP, du 27 février 2014, disponible à l'adresse:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp212_en.pdf.

103 Les tâches qui relèvent généralement toujours du contrôle direct de l'institution de l'UE sont notamment:

- Le respect de la protection des données en tant que responsable du traitement, notamment:
  - la gestion et l'évaluation/la réévaluation des risques liés à la protection des données;
  - les garanties de protection des données et les contrôles de sécurité des TI ainsi que la définition des objectifs et la gestion;
  - la gestion des demandes des personnes concernées;
  - la notification des violations de données à caractère personnel au CEPD et aux personnes concernées;
  - les audits de la protection des données auprès du fournisseur de services en nuage;
  - le DPD et son rôle.
- La gestion et la gouvernance des TI.
- La gestion des contrats.
- La gestion et la définition du niveau de service.
- La gestion et les contrôles des données (politiques et projets pour l'accès, le stockage, la suppression et la restitution des données par le fournisseur de services en nuage, par exemple).
- Les audits (de manière globale) du fournisseur de services en nuage.

Ces tâches nécessitent des ressources expérimentées adéquates, principalement dans la gestion des contrats, des finances, des TI, de la sécurité des TI et de la protection des données.

104 Des **ressources adéquates dans le domaine des TI** peuvent encore être nécessaires même dans le modèle de service SaaS dans les services publics en nuage, qui présente le niveau le plus élevé de délégation. Dans ce cas, si le personnel qui met en œuvre l'infrastructure de TI et le service spécifique n'est plus nécessaire, le personnel capable de comprendre et d'évaluer le caractère approprié de l'architecture des TI et les aspects liés à la conception ainsi que les mesures et les politiques en matière de sécurité des TI est toujours nécessaire afin de vérifier si la solution est adéquate au titre des exigences en matière de protection des données.

105 Les **politiques** et les **procédures** permettant de réaliser ces tâches doivent être **décrites et disponibles** en vue d'audits éventuels.

106 En ce qui concerne la gestion de contrat, par exemple, l'institution de l'UE devrait **tenir une liste des accords de sous-traitance notifiés par le fournisseur de services en nuage**, qu'elle devrait **mettre à jour au minimum une fois par an**. Cette liste est mise à la disposition du CEPD sur demande.

107 Le **DPD** de l'institution de l'UE est le membre du personnel qui conseille l'institution de l'UE sur la manière de respecter les principes et la législation en matière de protection des

données et qui fournit une assistance conformément à la législation[49]. Il devrait toujours **être associé d'une manière appropriée**, dès le début du processus et tout au long des différentes étapes, à la conception et à l'exploitation du service en nuage, notamment:

- lors de l'évaluation des risques liés à la protection des données, en définissant les exigences et les garanties pertinentes;
- si la réalisation d'une analyse d'impact relative à la protection des données constitue une exigence obligatoire;
- lors de la définition des clauses contractuelles ainsi que du contenu de l'accord de niveau de service;
- en cas de violations des données à caractère personnel;
- lors des audits de la protection des données.

108 L'institution de l'UE devrait également prévoir une **formation** appropriée sur les règles en matière de protection des données à caractère personnel pour son personnel concernant l'utilisation du service en nuage et le contrôle de la conformité de ce service avec les conditions sur la protection des données prévues dans le contrat. Les membres du personnel concernés par cette formation sont notamment: les décideurs, les responsables du processus, les gestionnaires de contrat, les personnes qui ont un accès permanent ou régulier aux données à caractère personnel, celles qui participent à la collecte et au traitement des données à caractère personnel et le personnel des TI participant au développement et à l'exploitation des outils utilisés pour traiter ces données.

109 L'institution de l'UE doit prévoir des **audits** éventuels, si elle l'estime nécessaire au regard des risques liés à l'opération de traitement, régulièrement ou lorsque des circonstances spécifiques l'exigent. Elle peut également réaliser ces audits par l'intermédiaire de **tiers** agréés aux fins des normes et certifications appropriées liées au service en nuage. Il est essentiel que:

- le programme d'audit comprenne tous les aspects des exigences en matière de protection des données à caractère personnel et fournisse des méthodes visant à garantir que des mesures correctives sont mises en place;
- les résultats de l'ensemble des audits soient communiqués au DPD et à la direction de l'institution de l'UE (par exemple, au directeur de l'agence de l'UE). Le CEPD reçoit un exemplaire de ces audits sur demande;
- le projet d'audit permette au CEPD d'être informé à l'avance, de participer à l'audit, s'il le décide, et de recevoir les résultats de l'audit.

4.3.2. L'accord de niveau de service

110 **L'accord de niveau de service fait partie du contrat et définit plus précisément les services attendus ainsi que leur niveau.** La décision de placer ces dispositions soit dans le

[49] Concernant le rôle (renforcé) du DPD conformément au RGPD, voir en particulier les articles 38 et 39.

texte principal du contrat, soit dans un accord de niveau de service, revient à l'institution de l'UE.

111 En outre, le contenu d'un accord de niveau de service dépend clairement du modèle de déploiement et de service, qui a un effet sur **l'attribution du contrôle direct et des responsabilités y afférentes** à l'institution de l'UE et au fournisseur de services en nuage.

112 L'accord de niveau de service devrait cibler et définir au minimum les domaines et éléments suivants[50]:

- Une **description détaillée du service fourni**.

  Cette description doit intégrer et détailler les éléments manquants dans le contrat. Les finalités des opérations de traitement des données à caractère personnel devraient, entre autres, être clairement définies.

- Une **répartition claire des responsabilités** (quant au niveau d'exploitation du service - qui fait quoi, y compris les mesures de sécurité) entre l'institution de l'UE et le fournisseur de services en nuage, à partir du niveau qui exerce un contrôle «de facto» sur la question.

- Les **canaux de communications** entre l'institution de l'UE et le fournisseur de services en nuage, notamment le service d'assistance de ce dernier.

- **Qualité/fourniture du service et notification:**

  Des définitions claires de la fourniture du service, du contrôle et de la notification doivent être convenues à l'aide d'indicateurs mesurables et d'outils de notification et de contrôle.

- **Capacité** requise.

  Cela désigne, par exemple pour le SaaS ou le PaaS, les cas et les environnements (de développement, de test, de production, etc.), l'espace de stockage, le nombre de comptes utilisateurs et administratifs, etc.

- **Disponibilité**

  Les objectifs de disponibilité, à des intervalles et des périodes de temps différents de l'année, ou une typologie d'utilisation, les indicateurs de disponibilité, le temps moyen entre les incidents de service, l'intervalle de maintenance, etc. La disponibilité devrait être définie pour tous les environnements demandés. Il est nécessaire d'apporter un soin spécifique à une définition commune pour éviter les malentendus.

- **Politique de sauvegarde, gestion des urgences, récupération après sinistre et continuité des activités.**

  Entre autres, les périodes de conservation de données doivent être définies en même temps que les mesures à appliquer aux données à l'expiration desdites périodes. Des procédures claires visant à restituer les données à tout moment, y compris le calendrier et le format des données, doivent être convenues et testées.

---

[50] Des orientations supplémentaires sur les accords de niveau de service en nuage peuvent être consultées dans les publications d'un consortium d'industries sous la coordination de la Commission européenne: «Cloud Service Level Agreement Standardisation Guidelines» - Cloud Select Industry Group - Bruxelles, 24 juin 2014, disponible à l'adresse:

https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines.

Ces orientations sectorielles ne doivent pas être considérées comme une source faisant autorité et ne reflètent pas nécessairement le point de vue du CEPD.

- **Gestion des changements**

  La procédure de gestion des changements qui sont pertinents pour le service en nuage (ceux requis par l'institution de l'UE, comme de nouvelles fonctionnalités, des modifications de l'accord de niveau de service et les changements que le fournisseur de services en nuage pourrait proposer, par exemple dans une offre IaaS) doit être définie et convenue de façon à ce que l'institution de l'UE ait le contrôle des procédures et des moyens de traitement des données.

- **Mesures de sécurité et niveaux d'assurance**

  L'institution de l'UE précise quelles garanties de sécurité le fournisseur de services en nuage doit mettre en place et vérifie le caractère adéquat de celles offertes par le fournisseur. Cela doit s'inscrire dans le cadre du résultat de l'analyse des risques liés à la protection des données réalisée et inclure:

  - la définition des objectifs de sécurité/niveaux/critères d'assurance, en se référant éventuellement aux normes et bonnes pratiques existantes;
  - la définition de contrôles/mesures de sécurité spécifiques.

  Le chiffrement efficace des données à caractère personnel, selon la nécessité, doit faire partie des mesures.

  Voir la section 4.4 pour plus d'informations sur les contrôles de sécurité possibles.

- **Garanties concernant la protection des données**

  L'institution de l'UE définit, dans l'accord de niveau de service, des dispositions spécifiques possibles, outre les mesures de sécurité, concernant la protection des données, en précisant davantage ou en ajoutant des garanties qui ne sont pas visées dans les clauses, le cas échéant.

- **Incidents de sécurité et violations de données à caractère personnel**

  Il convient de fournir davantage de détails (y compris les formes et les canaux de notification convenus) à ce qui est déjà prévu dans les clauses. Voir aussi la note de bas de page n°**Error! Bookmark not defined.**.

- **Contrôles et audits, y compris scientifiques**

  Le fournisseur de services en nuage doit consigner les opérations concernant les données à caractère personnel et les mettre à la disposition, si nécessaire, de l'institution de l'UE.

  Les caractéristiques et les rapports permettant à l'institution de l'UE d'avoir le contrôle doivent être définis, tout comme les modalités et les termes des audits/inspections des locaux du fournisseur de services en nuage et de ses centres de données par les institutions de l'UE et le CEPD.

  Si des analyses scientifiques par l'institution de l'UE ou le CEPD sont nécessaires, le fournisseur de services en nuage devrait avoir les capacités de coopérer d'une manière efficace et efficiente.

- **Résiliation du service et remise**

  Il convient de définir le calendrier et la prise en charge de la résiliation du service et de la transmission, y compris la restitution des données ou l'exportation vers un nouveau fournisseur de services en nuage. La prise en charge doit inclure la restitution des données ou leur remise à un nouveau fournisseur de services. Les procédures relatives à la suppression définitive au terme de la remise sont incluses. Les dispositions possibles relatives à la vérification nécessaire via l'inspection des locaux et des enregistrements doivent également être incluses.

- **Suppression et élimination sécurisées**

  Le fournisseur de services en nuage doit techniquement garantir des mécanismes d'élimination sécurisés, comme la destruction, la démagnétisation ou l'écrasement, et fournir à l'institution de l'UE un élément de preuve de la destruction réalisée, notamment des copies de sauvegarde.

- **Sanctions** en cas de non-respect de l'accord de niveau de service

  Outre le droit à une compensation en cas de préjudice subi à la suite d'une violation du contrat ou de l'accord de niveau de service par le fournisseur de services en nuage, l'institution de l'UE devrait avoir le droit de suspendre et/ou de résilier le contrat.

- Procédure de **révision de l'accord de niveau de service**

  Il devrait exister une procédure pour la révision de l'accord de niveau de service. En aucun cas, cependant, le fournisseur de services en nuage n'est autorisé à le modifier de manière unilatérale.

4.4. Mesures de sécurité des TI

113 Les mesures de sécurité et la responsabilité qui s'y rapporte devraient se refléter dans:

- le contrat (notamment l'accord de niveau de service), pour les mesures qui sont sous le contrôle et l'exploitation du fournisseur de services en nuage, ou
- les procédures/la politique interne(s), pour autant qu'elles soient sous le contrôle direct de l'institution de l'UE.

114 Une **liste** non exhaustive **des mesures de sécurité des TI possibles** atténuant les risques spécifiques aux services d'informatique en nuage figure ci-après à la recommandation **R2** relative à ces risques. Les risques sont indiqués conformément à la liste de risques à l'Annexe 4. D'autres garanties non liées aux TI sont également décrites, pour illustrer la méthode fondée sur le risque, qui atténue les mêmes risques avec différentes incidences.

115 La valeur de leur pouvoir d'atténuation, le cas échéant, n'est pas absolue, mais elle vise simplement à classer l'efficacité des différentes garanties en situation «moyenne».

116 La liste complète de garanties devrait être le résultat de l'évaluation des risques liés à la protection des données, y compris d'une évaluation des risques liés à la sécurité des informations[51] (qui, bien sûr, tiendra également compte des risques pour les systèmes d'information externalisés).

117 Dans tous les cas, il est recommandé de se référer aux pratiques et politiques internes existantes en matière de sécurité des TI dans les institutions de l'UE et aux bonnes pratiques et normes disponibles en matière de sécurité des TI publiées par le secteur ainsi que par d'autres organisations, telles que l'Organisation internationale de normalisation ainsi que

[51] Pour plus d'informations, consulter les orientations du CEPD intitulées «Security Measures for Personal Data Processing» (mesures de sécurité pour le traitement des données à caractère personnel): https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-03-21_Guidance_ISRM_EN.pdf ainsi qu'une lettre du CEPD visant à clarifier le lien entre l'analyse d'impact relative à la protection des données et la gestion des risques liés à la sécurité des informations:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Accountability/16-04-22_Mail_DPOs_WW_EN.pdf.

l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA). Voir également Annexe 5 pour un certain nombre de références.

R2 - Confidentialité et risques liés à l'intégrité pour les données en transit sur l'internet

Le service demandé sera situé en dehors du centre de données de l'institution de l'UE et ne sera pas accessible par des lignes louées. Un autre moyen de communication doit être fourni, très probablement l'internet, comme pour la plupart des fournisseurs de services en nuage.

Parmi les garanties possibles:

- avoir uniquement recours aux fournisseurs de services en nuage qui offrent des lignes dédiées permettant de se connecter à leurs services + un chiffrement efficace;

  Pouvoir d'atténuation: élevé, très élevé

- mettre en œuvre des réseaux privés virtuels (VPN) sur l'internet, en utilisant éventuellement le chiffrement et l'authentification également au niveau multiprotocoles;

  Pouvoir d'atténuation: élevé

- utiliser un chiffrement puissant (par exemple HTTPS avec mise en œuvre du TLS);

  Pouvoir d'atténuation: moyen-élevé

R3 - Indisponibilité éventuelle liée à une absence d'accès à l'internet ou à un accès limité à celui-ci

Parmi les garanties possibles:

- fournisseurs internet multiples avec permutation à chaud;

  Pouvoir d'atténuation: élevé

- lignes redondantes à partir du même fournisseur;

  Pouvoir d'atténuation: moyen-élevé

- ne pas utiliser l'internet, mais des lignes louées, pour faire le lien entre l'utilisateur et le fournisseur de services en nuage;

  Pouvoir d'atténuation: très élevé

R4 - Risques liés à la surveillance internet (fournisseurs de service internet + dorsale internet et infrastructure d'acheminement)

Parmi les garanties possibles:

- limiter les fournisseurs de services en nuage éventuels aux pays de l'UE;

  Pouvoir d'atténuation: moyen-élevé

- ne pas utiliser l'internet, mais des lignes louées, pour faire le lien avec le fournisseur de services en nuage, toujours au sein du territoire de l'UE;

  Pouvoir d'atténuation: très élevé

- utiliser un chiffrement de bout en bout (par exemple HTTPS avec mise en œuvre du TLS);

  Pouvoir d'atténuation: élevé

R6 Vulnérabilités possibles dans les politiques d'accès et les contrôles de sécurité

Ce risque est particulièrement présent s'il y a plusieurs utilisateurs: nuage public ou communautaire.

Parmi les garanties possibles:

- demander au fournisseur de services en nuage de fournir des preuves de la mise en œuvre de mesures de sécurité efficaces pertinentes qui seraient adaptées à la nature des données à caractère personnel traitées, par:
    - une déclaration sur l'honneur de conformité avec les bonnes pratiques et les normes en matière de sécurité en nuage;

      Pouvoir d'atténuation: faible
    - la fourniture d'une assurance par des tiers agréés (certification de sécurité en nuage remédiant au risque et adaptée à la nature des données à caractère personnel traitées);

      Pouvoir d'atténuation: moyen/élevé, selon la fiabilité du mécanisme de certification

      Cette assurance devrait être apportée tout au long de la fourniture du service et lors de la résiliation du service et de la transmission.
- demander au fournisseur de services en nuage d'isoler l'environnement informatique des autres utilisateurs:
    - isolation physique, comme le recours à différents serveurs pour différents utilisateurs;

      Pouvoir d'atténuation: élevé
    - utiliser différentes machines virtuelles au sein du même serveur pour différents utilisateurs;

      Pouvoir d'atténuation: moyen
- chiffrement adéquat des données au repos et en transit dans l'infrastructure en nuage au sein de différents périmètres de sécurité. La solidité du chiffrement et du mécanisme de gestion des clés devrait être déterminée sur la base de l'analyse des risques. La possibilité de garder les données chiffrées lors de leur traitement fait toujours l'objet de recherches, mais l'institution de l'UE est invitée à vérifier l'évolution de cette technique. Si les clés chiffrées sont gérées par le fournisseur de services en nuage, des mesures de sécurité adéquates visant à les protéger sont essentielles à l'efficacité du chiffrement[52].

  Pouvoir d'atténuation: élevé, très élevé si associé à une bonne isolation des données des autres propriétaires

[52] Les documents de l'ENISA pourraient, entre autres, être utilisés pour évaluer les clés et les algorithmes de chiffrement:

- Study on cryptographic protocols (étude sur les protocoles de chiffrement) et Algorithms, key size and parameters report 2014 (rapport 2014 sur les algorithmes, la taille des clés et les paramètres).

R12 - Absence de contrôle adéquat (par l'institution de l'UE ou les tiers désignés) et d'activités de contrôle et d'enquête par les autorités compétentes, y compris scientifiques

L'institution de l'UE devrait veiller à ce que le fournisseur de services en nuage garantisse un niveau approprié de contrôle pour pouvoir démontrer, sur demande, sa conformité et répondre de manière efficace et efficiente à des demandes d'enquête. Quelques conditions préalables:

- tout traitement des données à caractère personnel doit être enregistré de manière sécurisée afin de vérifier les responsabilités et les opérations de traitement et ces enregistrements doivent être mis à la disposition de l'institution de l'UE pour des vérifications. Ces enregistrements doivent être protégés par les mêmes mesures que les données à caractère personnel d'origine;
- développement d'une capacité technique permettant de gérer et d'analyser ces enregistrements.

Parmi les garanties possibles:

- l'institution de l'UE ou tout tiers agissant pour le compte de celle-ci réalise des audits périodiques de l'infrastructure du fournisseur de services en nuage touchant le service demandé;

  Pouvoir d'atténuation: en principe très élevé, mais cela dépend de la capacité d'audit et de la complexité de l'infrastructure de TI du fournisseur de services en nuage

- le fournisseur de services en nuage doit fournir des preuves des audits réalisés périodiquement par des tiers agréés/faisant l'objet d'une confiance mutuelle. L'accréditation du tiers devrait se faire conformément à une certification/norme fiable relative au nuage, qui répond aux risques pertinents et qui est adaptée à la nature des données à caractère personnel traitées;

  Pouvoir d'atténuation: élevé

- le fournisseur de services en nuage fournit des preuves des audits internes/auto-évaluations réalisé(e)s périodiquement, répondant aux risques pertinents et adaptés à la nature des données à caractère personnel traitées.

  Pouvoir d'atténuation: faible, moyen si cela s'inscrit dans le cadre d'un code de conduite reconnu

R14 - Enfermement propriétaire éventuel (vente ou arrêt de l'activité, en raison d'une faillite ou autre): données indisponibles ou politique en matière de vie privée/législation applicable différente

Parmi les garanties possibles:

- concevoir et tester périodiquement une procédure de rechange pour prendre en charge les processus d'activité ciblés de l'institution de l'UE. Une sauvegarde périodique en dehors des locaux du fournisseur de services en nuage (soit dans les locaux de l'institution de l'UE, soit par un autre fournisseur) doit être réalisée afin de minimiser les éventuelles pertes de données;

  Pouvoir d'atténuation: élevé

- concevoir et tester un plan de migration afin de changer de fournisseur de services en nuage.

  Pouvoir d'atténuation: nécessaire, mais pas suffisant

R18 - Autres risques liés à la sécurité des TI spécifiques à l'informatique en nuage (voir également Annexe 4).

Nous fournissons ici un exemple. Pour tous les autres risques liés à la sécurité des TI spécifiques à l'informatique en nuage, nous vous invitons à consulter le responsable de la sécurité et les références spécialisées comme à l'Annexe 5.

Vulnérabilités liées à l'utilisation du logiciel client

Le service en nuage peut entraîner l'utilisation de clients (généralement légers) comme des navigateurs commerciaux ou d'autres clients ou des applications mobiles développées par le fournisseur de services en nuage. Cela peut entraîner des risques éventuels en raison des vulnérabilités de l'agent client. Il ne s'agit pas simplement d'un risque spécifique au nuage, cela pourrait être une modification concernant le système de TI actuellement utilisé et donc comporter de nouveaux risques, qui pourraient avoir une incidence également sur d'autres systèmes et données à caractère personnel gérés par l'institution de l'UE.

Parmi les garanties possibles:

- lors du choix et de la configuration du navigateur, l'institution de l'UE devrait accorder une attention spécifique à ses faiblesses/aspects liés à la vie privée, tels que:
    - le chiffrement du canal pour les communications HTTP et en particulier la prise en charge de clés de chiffrement et de protocoles fiables;
    - toutes autres opérations de traitement des données transmises/reçues qui ne sont pas nécessaires pour l'utilisation du service en nuage (y compris les transferts de données aux destinataires autres que le service en nuage);
- l'institution de l'UE pourrait envisager d'utiliser des navigateurs dédiés au service en nuage afin que l'incidence des attaques provenant d'autres sites web soit limitée. Une mesure plus solide pourrait être l'utilisation d'un bureau virtuel connecté à un serveur sécurisé dédié à distance sur lequel le navigateur dédié est installé;
- si le fournisseur de services en nuage fournit son propre client afin de se connecter au service en nuage, l'institution de l'UE devrait demander que le fournisseur gère de manière adéquate les risques en matière de sécurité liés au client;
- une attention particulière devrait être portée à la gestion de la sécurité des applications mobiles en tant que clients en nuage[53], en raison des risques spécifiques qu'elles comportent[54];
- l'institution de l'UE devrait installer dans les meilleurs délais les mises à jour de sécurité des entreprises de navigateurs commerciaux ou du fournisseur de services en nuage.

[53] Voir «EDPS guidelines on the protection of personal data processed by mobile applications provided by EU institutions and bodies» (Lignes directrices du CEPD sur la protection des données à caractère personnel dans les dispositifs mobiles utilisés par les institutions et les organes de l'UE), disponibles à l'adresse;

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/16-11-07_Guidelines_Mobile_apps_EN.pdf.

[54] Voir également l'avis du groupe de travail «Article 29» (WP202) sur les applications destinées aux dispositifs intelligents, disponible à l'adresse:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

Annexe 1. Glossaire

Terme	Description
Authentification	Le processus visant à garantir et à confirmer l'identité d'un utilisateur ou d'une machine réalisant une opération (généralement par l'intermédiaire d'un système de TI).
Clés de chiffrement	Informations généralement utilisées pour chiffrer (ou déchiffrer) des données d'une manière unique. À cet effet, elles constituent le «secret» permettant finalement la divulgation sélective des données uniquement aux personnes qui connaissent ce secret.
Réseaux privés virtuels (VPN)	Un VPN est une connexion sécurisée (chiffrée) point à point généralement établie sur un réseau public.
Fournisseur de services en nuage	Un fournisseur de services de TI basés sur le nuage.
Données à caractère personnel	Toute information se rapportant à une personne physique identifiée ou identifiable («personne concernée»); une personne physique identifiable est une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
Catégories particulières (de données à caractère personnel)	Au titre du règlement actuel, il s'agit des données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé ou à la vie sexuelle. La proposition de nouveau règlement ajoute les données génétiques et biométriques afin d'identifier de façon unique une personne physique. Ces catégories sont soumises à des règles spécifiques.
Responsable du traitement	L'institution ou organe communautaire, la direction générale, l'unité ou toute autre entité organisationnelle qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.
Sous-traitant	Personne physique ou morale, autorité publique, agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.
Sous-traitant ultérieur	Personne physique ou morale, autorité publique, agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du sous-traitant.

Délégué à la protection des données (DPD)	Membre du personnel d'une organisation chargé de soutenir l'organisation en garantissant le respect de la législation applicable en matière de protection des données. Sa nomination, ses tâches et ses pouvoirs sont définis dans le règlement (et dans le nouveau règlement).
Personne concernée	Individu dont les données à caractère personnel sont traitées.
Clauses contractuelles types	Clauses à utiliser dans les contrats passés entre le responsable du traitement et le sous-traitant ou entre un sous-traitant et un autre sous-traitant agissant en tant que sous-traitant ultérieur, au sens du règlement (et de la proposition de nouveau règlement), adoptées par la Commission européenne ou par une autorité de contrôle conformément aux procédures prévues dans la législation et fournissant l'assurance contractuelle nécessaire.
Règles d'entreprise contraignantes	Règles incluant l'ensemble des principes essentiels et des droits opposables devant être appliqués par un groupe d'entreprises pour les transferts internationaux de données à caractère personnel à partir d'organisations de l'Union au sein du même groupe d'entreprises pour veiller au recours aux garanties appropriées prévues par la législation.
Analyse d'impact relative à la protection des données	Analyse des risques pour les droits et les libertés des personnes physiques posés par le traitement de leurs données à caractère personnel. Le nouveau règlement prévoit des éléments obligatoires et des circonstances dans lesquelles l'analyse est obligatoire. Toutefois, les responsables du traitement peuvent réaliser cette analyse et obtenir des avantages intéressants en dehors de ces circonstances.
Contrat-cadre	Le contrat-cadre est un modèle de contrat associé à une procédure de passation de marchés publics, qui, une fois le marché attribué, doit être instancié davantage sous la forme de «contrats spécifiques» afin de préciser davantage et définitivement les termes contractuels pour la fourniture de services ou de produits.
Contrat spécifique	Voir la définition de «contrat-cadre».
Accord de niveau de service (SLA)	Engagement officiel, faisant souvent partie des contrats et définissant la qualité des services rendus par le fournisseur au client. Par exemple, la disponibilité mensuelle minimale moyenne d'un service en nuage peut être un élément défini dans un accord de niveau de service.
Certification	Confirmation du respect des normes/bonnes pratiques par les tiers agréés. Les certifications sont un élément parmi d'autres qui aident les fournisseurs de services en nuage à garantir le respect des nouvelles règles en

	matière de protection des données selon ce qui est prévu dans la législation.
Code de conduite	Un ensemble de règles définies par des personnes ou des entreprises qui peuvent les utiliser pour s'engager à faire plus que ce que la législation impose ou pour mettre en œuvre ce que la législation impose. Les codes de conduite sont un élément parmi d'autres qui aident les fournisseurs de services en nuage à garantir le respect des nouvelles règles en matière de protection des données selon ce qui est prévu dans la législation.
Machine virtuelle	Une machine virtuelle est un ordinateur «virtuel» qui est exécuté sur un ordinateur physique, doté de son propre système d'exploitation, de ses propres dispositifs et applications, isolé d'autres machines virtuelles exécutées sur le même ordinateur physique. Ce phénomène est possible grâce à une application logicielle de «virtualisation» fonctionnant sur cet ordinateur.

Annexe 2. Analyse juridique supplémentaire

La présente annexe fournit certains autres éclairages et raisonnements juridiques pour compléter les orientations données dans les chapitres, sans prétendre à l'exhaustivité.

Ci-après, nous présentons brièvement certaines raisons (**outre celle concernant l'applicabilité du protocole sur les privilèges et immunités de l'Union européenne**) à l'appui de **la recommandation** formulée au paragraphe 63 des présentes lignes directrices, à savoir que le traitement des données à caractère personnel confié par les institutions de l'UE aux fournisseurs de services en nuage, et à leurs éventuels sous-traitants ultérieurs, a lieu, **en règle générale**, **au sein de l'UE**[55].

1) La localisation du fournisseur de services en nuage et de son centre de données et/ou de ses serveurs hors de l'UE est un facteur qui, *entre autres*, détermine l'applicabilité ou non de la législation d'un pays tiers (question de l'applicabilité de la compétence et la législation d'un pays tiers).

Des exemples concernant **différents domaines de la législation** (autres que la législation en matière de protection des données) pourraient être mentionnés brièvement, comme suit:

i) En ce qui concerne l'application de la **législation pénale**, nous rappelons que l'accès des autorités répressives d'un pays tiers à un centre de données **situé dans un État membre de l'UE** nécessiterait, en règle générale, une demande de ces autorités auprès de l'État membre conformément à un accord international spécifique, un traité d'entraide judiciaire ou un protocole d'accord, établissant des garanties adéquates en matière de protection des données[56]. Ce type de demande au titre d'un traité d'entraide judiciaire ne serait **pas** requis dans le cas d'un accès des autorités répressives d'un pays tiers à un centre de données situé sur leur propre territoire.

---

[55] Le traitement en dehors de l'UE devrait être *une exception* (par exemple, dans le cas d'un traitement de données présentant un faible risque) et, dans ce cas, l'institution de l'UE décrit et justifie la nécessité de ces opérations de traitement, en portant une attention particulière aux éventuels risques liés à la protection des données et aux risques liés à un contrôle efficace par l'autorité de contrôle.

Dans ce cas, les règles relatives aux transferts de données à caractère personnel à des pays tiers s'appliqueraient également. Pour des orientations sur les transferts de données à caractère personnel à des pays tiers et à des organisations internationales, sur la base de l'actuel règlement (CE) nº 45/2001, veuillez consulter le document d'orientation du CEPD «Orientations sur les transferts à des pays tiers et à des organisations internationales: article 9», y compris les cas pertinents du CEPD, disponible à l'adresse:

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_FR.pdf.

Veuillez noter toutefois que le document susmentionné du CEPD sera actualisé afin de tenir compte des dispositions révisées de la proposition de règlement sur les transferts internationaux de données à caractère personnel.

[56] Dans l'affaire «Microsoft Ireland», la Cour d'appel des États-Unis pour le deuxième circuit a décidé le 14 juillet 2016 que la législation américaine (Stored Communication Act, SCA) «*n'autorise pas un tribunal américain à délivrer et à appliquer un mandat au titre de la SCA à l'encontre d'un fournisseur de services établi aux États-Unis concernant les contenus des communications électroniques d'un client stockées sur des serveurs situés hors des États-Unis. En l'espèce, le mandat au titre de la SCA ne saurait être licitement utilisé pour contraindre Microsoft à fournir au gouvernement les contenus du compte de l'adresse électronique d'un client stocké uniquement en Irlande*». La Cour d'appel des États-Unis mentionne entre autres le critère «*locus rei sitae*». Le jugement est disponible à l'adresse suivante: http://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412.

Dans le même temps, rappelons que la **Convention sur la cybercriminalité** (Convention de Budapest)[57], garantie commune s'appliquant également aux pays tiers qui sont parties à la Convention, prévoit, en son article 15, que «[c]haque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures [en matière d'enquêtes pénales] [...] [intègrent] le principe de la **proportionnalité**».

ii) En vertu du **droit procédural en matière civile**, un centre de données situé dans un État membre de l'UE (et donc soumis, d'après le principe général de territorialité, au droit procédural en matière civile de cet État membre) ne peut faire l'objet d'une perquisition au titre de poursuites civiles – en droit américain, il est question de «**pre-trial discovery**» (c'est-à-dire la divulgation obligatoire d'informations qui peuvent en elles-mêmes ne pas être directement pertinentes, mais pourraient mener à la découverte d'informations importantes avant le procès). Dans ce cas, comme le recommande le groupe de travail «Article 29», les demandes de divulgation devraient préférablement être faites en appliquant la Convention de La Haye sur l'obtention des preuves à l'étranger en matière civile ou commerciale, selon laquelle «une procédure type est prévue pour l'émission de "commissions rogatoires" qui sont des requêtes formulées par le tribunal d'un pays auprès de l'autorité centrale désignée d'un autre pays demandant son assistance pour obtenir des renseignements utiles se trouvant sur son territoire». En revanche, un centre de données situé aux États-Unis peut être perquisitionné dans le cadre de cette procédure d'échange d'informations avant le procès (conservation des données, «litigation hold») en vertu des compétences prévues dans la législation applicable aux États-Unis et conformément à cette législation.[58]

iii) En ce qui concerne l'activité des **services nationaux de renseignement**, nous soulignons que: «Tous les États membres [de l'UE] sont parties à la "Convention européenne des droits de l'homme" [CEDH]. Ils doivent dès lors satisfaire aux conditions établies par l'article 8 de la CEDH concernant leurs propres **programmes de surveillance**. [...]. L'article premier de la CEDH dispose également que les parties doivent reconnaître à toute personne relevant de leur juridiction les droits et libertés définis dans la Convention. Dans les deux cas, les **États membres de l'Union, à l'instar de toutes les parties à la CEDH**, peuvent être traduits devant la Cour européenne des droits de l'homme s'ils enfreignent le droit au respect de la vie privée dont jouit tout sujet de droit européen».[59]

---

[57] La **Convention sur la cybercriminalité** du Conseil de l'Europe (série des traités européens nº 185), connue sous le nom de Convention de Budapest, est disponible à l'adresse: http://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185.

[58] Voir le document de travail du groupe de travail «Article 29» 1/2009 sur la **procédure d'échange d'informations avant le procès («pre-trial discovery») dans le cadre de procédures civiles transfrontalières**, disponible à l'adresse:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_fr.pdf.

[59] Avis 04/2014 du groupe de travail «Article 29» sur la surveillance des communications électroniques à des fins de **renseignement et de sécurité nationale**,disponible à l'adresse:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_fr.pdf.

Dans ses résolutions du 10 décembre 2013 sur l'informatique en nuage et du 12 mars 2014 sur la surveillance, le Parlement européen a réaffirmé ses préoccupations concernant en particulier l'accès par les services de renseignement de pays tiers à des fournisseurs d'informatique en nuage utilisant des serveurs de stockages situés dans des pays tiers.

Voir également l'étude réalisée par l'Agence des droits fondamentaux de l'Union européenne (FRA) intitulée «Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU», disponible à l'adresse: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2016-surveillance-intelligence-services_en.pdf.

Ce rapport cartographie les cadres juridiques relatifs à la surveillance en place dans les États membres de l'UE. Il présente aussi en détail les mécanismes de contrôle mis en place à travers l'UE, souligne les travaux des entités

Ces garanties ne s'appliquent **pas** aux États qui ne sont **pas** partie à la CEDH (la liste des États qui ont signé et ratifié la CEDH est disponible à l'adresse: https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/005/signatures?p_auth=55fMgptN). Tous les États membres de l'Union européenne sont parties à la CEDH.

En substance, le stockage et le traitement de données dans un centre de données ou par une entreprise située sur le territoire d'un pays donné justifient généralement la compétence de l'organisme public de ce pays pour demander l'accès aux données traitées dans ledit centre de données dans le contexte d'une mesure d'exécution **du droit public** de ce pays (par exemple droit pénal, droit procédural, législation en matière de rétention de données, etc.). L'institution de l'UE doit analyser ce **risque** avec attention.

2) En outre, il convient de rappeler la **jurisprudence** récente de la Cour de justice de l'Union européenne (CJUE):

Dans l'**«arrêt sur la conservation des données»** [60], la CJUE souligne (au point 68) la circonstance selon laquelle: «*la directive [relative à la conservation des données] n'impose pas que les données en cause soient conservées sur le territoire de l'**Union**, de sorte qu'**il ne saurait être considéré qu'est pleinement garanti le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité** [...]. Or, un tel **contrôle**, effectué sur la base du **droit de l'Union**, constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel*» (*caractères gras ajoutés*).

Dans l'«**arrêt Schrems»**[61], la CJUE a également souligné qu'un **contrôle efficace** effectué par des autorités de contrôle exerçant en toute indépendance, jouissant de tous les pouvoirs dont elles sont investies, est un élément essentiel de la protection des données à caractère personnel.

De la même manière, dans l'«**arrêt Tele2**[62]», la CJUE a déclaré (au point 122), que: «En ce qui concerne les règles visant la **sécurité et la protection des données** conservées par les fournisseurs de services de communications électroniques, il convient de constater que l'article 15, paragraphe 1, de la directive 2002/58 ne permet pas aux **États membres** de déroger à l'article 4, paragraphe 1, ainsi qu'à l'article 4, paragraphe 1 *bis*, de celle-ci. Ces dernières dispositions exigent que ces fournisseurs prennent les mesures d'ordre technique et organisationnel appropriées permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès illicite à ces données. Compte tenu de la **quantité** de données conservées, du **caractère sensible** de ces données ainsi que du **risque d'accès illicite** à celles-ci, les fournisseurs de services de communications électroniques doivent, aux fins d'assurer la pleine intégrité et la confidentialité desdites données, garantir un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles appropriées. En particulier, la réglementation nationale doit prévoir la **conservation sur le territoire de l'Union** ainsi que la destruction irrémédiable des données au terme de la durée de conservation de celles-ci» (*caractères gras ajoutés*).

---

chargées de contrôler les opérations de surveillance et expose les voies de recours à la disposition des citoyens qui souhaitent s'opposer à ces activités de renseignement.

[60] Arrêt de la Cour du 8 avril 2014 dans les affaires jointes Digital Rights Ireland et Seitlinger e.a., C-293/12 et C-594/12.

[61] Arrêt de la Cour (grande chambre) du 6 octobre 2015 dans l'affaire Maximillian Schrems/Data Protection Commissioner, C-362/14 [ayant pour objet une demande de décision préjudicielle introduite par la High Court (Haute Cour de justice, Irlande)].

[62] Arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016 dans les affaires jointes *Tele2 Sverige AB/Post-och telestyrelsen et Secretary of State for the Home Department/Tom Watson e.a.*, C-203/15 et C-698/15.

3) Si la localisation de l'hébergement de l'architecture en nuage est située dans un pays tiers, il pourrait être **plus difficile pour le CEPD de coopérer et de coordonner les inspections** avec les autres autorités nationales chargées de la protection des données dans l'Union et donc de garantir l'application globale des dispositions du règlement**3)** .

Par conséquent, au vu de ce qui précède, **le CEPD recommande, *en règle générale*, que le traitement des données à caractère personnel confié par les institutions de l'UE aux fournisseurs de services en nuage (y compris à des fins de sauvegarde, de continuité des activités et de transit, ainsi que les localisations à partir desquelles des opérations à distance sont réalisées), *et à leurs sous-traitants ultérieurs*, se déroule au sein de l'UE**.

Annexe 3. Modèles et concepts de base de l'informatique en nuage

Définition de l'informatique en nuage

Les technologies et services d'informatique en nuage peuvent être mis en œuvre dans un vaste ensemble d'architectures, sous différents modèles de service et de déploiement. Le terme revêt différentes significations dans des contextes variés. La définition la plus couramment utilisée est celle du US National Institute of Standards and Technology (NIST)[63], qui indique que l'informatique en nuage est un modèle permettant d'accéder partout, aisément et à la demande, par le réseau, à des ressources informatiques configurables partagées (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement mobilisées et libérées avec un minimum d'effort de gestion ou d'intervention d'un prestataire de services. Le document du NIST définit trois modèles de services (SaaS: Software as a Service ou logiciel en tant que service; PaaS: Platform as a Service ou plateforme en tant que service; et IaaS: Infrastructure as a Service ou infrastructure en tant que service) et quatre modèles de déploiement: les environnements en nuage publics, privés, communautaires et hybrides (une composition des trois modèles précédents). Dans les présentes lignes directrices, les termes et acronymes utilisés ont le sens qui leur est donné par cette définition.

Comme nous l'avons dit précédemment, les présentes lignes directrices sont axées sur les environnements en nuage publics étant donné qu'ils présentent des défis spécifiques en matière de protection des données à caractère personnel. Les services en nuage hybrides faisant intervenir des infrastructures en nuage publiques et privées sont également abordés en raison de l'aspect public et de leur interaction avec des infrastructures privées lors de la prestation des services.

Externalisation traditionnelle et informatique en nuage

Le recours à des services en nuage publics constitue effectivement un nouveau mode d'externalisation. Il se produit lorsqu'une organisation qui traitait ses données dans son propre centre de données décide d'avoir recours à un service fondé sur le nuage. Cela comporte à la fois les risques liés à l'externalisation traditionnelle et les risques spécifiques à l'informatique en nuage, lesquels sont traités à l'Annexe 4. L'informatique en nuage n'est donc pas «simplement un mode d'externalisation supplémentaire» et appelle une analyse et des garanties spécifiques.

Il convient de noter que certaines entreprises de TI promeuvent des services disponibles sur l'internet comme étant fondés sur le nuage, même s'ils ne répondent pas aux critères d'un service en nuage, comme:

- l'autoapprovisionnement en capacités informatiques sur demande, comme l'heure du serveur et le stockage en réseau;
- l'approvisionnement et la flexibilité faciles et rapides des ressources, avec un modèle de paiement à l'utilisation;
- un large accès à l'internet avec des agents utilisateurs et clients standard (par exemple, des navigateurs);
- la mise en commun des ressources dynamiquement réparties des fournisseurs afin de servir plusieurs utilisateurs en nuage, sans connaissance et/ou contrôle de l'utilisateur sur la localisation des ressources;

[63] US NIST SP 800-145, The NIST Definition of Cloud Computing (Définition de l'informatique en nuage du NIST), septembre 2011. Lien: https://csrc.nist.gov/publications/detail/sp/800-145/final.

- l'optimisation fluide des ressources mesurées allouées par le fournisseur de services.

En effet, les services offerts sur l'internet ne possèdent pas tous ces caractéristiques, qui peuvent également être présentes à différents degrés, en fonction notamment du modèle de service. En outre, il apparaît que les modèles de déploiement privés, communautaires et autres modèles de proximité conservent ou abandonnent des caractéristiques spécifiques au nuage sur la base de leur spécificité. Les risques spécifiques à l'informatique en nuage sont liés à ces caractéristiques, à la façon dont elles ont été mises en œuvre et à la manière dont les entreprises et les services d'informatique en nuage se sont développés.

Exemples de services en nuage accessibles au public

Même si tous les services de TI peuvent aujourd'hui être déployés dans un environnement en nuage, il apparaît que certains exemples de services fondés sur le nuage pourraient être intéressants pour les institutions de l'UE, pour rendre la pertinence du sujet discuté et les risques inhérents à celui-ci. En voici une liste non exhaustive:

- SaaS: services de stockage de données de base, suites bureautiques, services de gestion de documents et du flux de travail, applications de gestion du personnel, plateformes de gestion des dispositifs mobiles.
- PaaS: infrastructure logicielle, telle que des serveurs virtualisés dotés de systèmes d'exploitation spécifiques et d'une pile de logiciels connexes de base, par exemple des serveurs web et d'application, des bases de données, un environnement de langages de programmation fréquemment utilisés et autres outils. Un ensemble de machines virtuelles fondées sur Linux avec une pile de logiciels pertinents et des bases de données à accès libre et des utilitaires logiciels constituent un exemple de ce que les institutions de l'UE pourraient utiliser pour déployer et exploiter, par exemple, des sites web.
- IaaS: infrastructure informatique composée de machines virtuelles, d'infrastructures réseau et de stockage, y compris de dispositifs de sécurité, dans laquelle, en principe, toutes sortes de services logiciels sur n'importe quelle plateforme peuvent être déployés ou exploités. Les institutions de l'UE pourraient utiliser les services IaaS pour remplacer leur propre centre de données.
- Hybride: une institution de l'UE pourrait souhaiter utiliser une technologie qui équilibre la charge de manière fluide ou qui permet une allocation dynamique des ressources en nuage publiques pour intégrer et enrichir sa propre infrastructure de stockage ou infrastructure informatique.

Ces éléments peuvent être fournis soit par un fournisseur de services en nuage commercial, soit par une infrastructure «en nuage privée (ou communautaire) externalisée» (où les machines sont externalisées par l'institution de l'UE à une entreprise d'hébergement dans une configuration en nuage), voire par une infrastructure en nuage entièrement privée ou communautaire possédée par une ou plusieurs institutions de l'UE[64].

[64] Voir la référence de la note de bas de page précédente pour une description plus détaillée des modèles de déploiement possibles.

Annexe 4. Risques de l'informatique en nuage spécifiques à la protection des données

Dans la présente section, nous définissons les risques de haut niveau que comporte l'utilisation des services d'informatique en nuage. Tout d'abord, nous proposons une liste des risques liés aux caractéristiques générales de l'informatique en nuage d'une infrastructure en nuage publique. Ces risques sont ensuite analysés plus en profondeur pour des types de services en nuage spécifiques, sur la base d'autres modèles de déploiement et de service existants (voir Annexe 3, et une analyse relative est effectuée concernant les autres modèles).

Ces risques doivent être intégrés et éventuellement détaillés davantage dans une analyse d'impact relative à la protection des données (voir la section 4.1) dans laquelle toutes les menaces et vulnérabilités possibles ayant une incidence sur les données à caractère personnel sont envisagées et toutes les exigences de conformité sont prises en considération.

Chaque caractéristique spécifique de l'informatique en nuage comporte des risques pertinents liés à la protection des données. Certaines caractéristiques en nuage peuvent ensemble poser ou renforcer certains risques.

- *Cx – description de la caractéristique relative à l'informatique en nuage*
  - *Rx – description du risque*

- ***C1 - L'institution de l'UE n'a jamais utilisé de services fondés sur le nuage ou a une expérience très limitée en la matière.***
  - **R1 - L'absence d'expérience préalable suffisante dans l'attribution de services d'informatique en nuage** pourrait mener à sous-estimer les risques ou à choisir des garanties inappropriées. S'appuyer sur les services en nuage pour les processus liés aux activités institutionnelles principales ou pour traiter des données sensibles sans expertise pourrait mettre en péril les responsabilités et les tâches institutionnelles liées à la protection des données et avoir des conséquences sur les personnes concernées.
- ***C2 - Les services sont offerts via l'internet**, ce qui représente le moyen de communication habituel entre les fournisseurs de services en nuage et les utilisateurs du nuage. Cela représenterait un changement pour l'institution de l'UE qui, en général, traite ses données dans son propre centre de données ou dans celui d'une autre institution de l'UE (par exemple la DG DIGIT de la Commission européenne) généralement connecté par l'intermédiaire de moyens de communication dédiés à cette fin.*
  - **R2 - Risques liés à la confidentialité et à l'intégrité des données en transit sur l'internet**. Les liens internet entre le fournisseur de services en nuage et l'utilisateur du nuage peuvent permettre des accès non autorisés et la modification des données en transit, y compris dans les infrastructures mobile et fixe pour accéder aux fournisseurs de service internet (FSI). L'accès non autorisé aux données à caractère personnel peut avoir pour conséquence que les données seront utilisées pour des finalités différentes de celles autorisées et convenues et provoquer un préjudice à la protection des données et aux droits en matière de vie privée des personnes concernées.
  - **R3 - Manque de disponibilité** lié à un accès internet limité ou à une absence d'accès internet en raison d'une mauvaise planification de la capacité, d'une

éventuelle indisponibilité du fournisseur de service internet, d'un encombrement du réseau, d'attaques informatiques, etc. Dans ce cas, l'institution de l'UE et les personnes concernées ne seraient pas en mesure d'accéder à leurs données.

- **R4 - Surveillance internet par les gouvernements et les services de sécurité** dirigée vers les fournisseurs de service internet, la dorsale internet et l'infrastructure d'acheminement. Certaines données à caractère personnel traitées par l'institution de l'UE pourraient présenter un intérêt pour les gouvernements et les services de sécurité des pays traversés par les segments internet éventuellement utilisés pour se connecter au futur fournisseur de services en nuage.
- **R5 - Des dispositions juridiques intrusives en matière de conservation des données à des fins d'application de la législation** applicable aux fournisseurs de services en nuage et aux fournisseurs de service internet pourraient accroître la période de conservation habituelle et ainsi augmenter la probabilité d'éventuels abus et fuites de données. Cette situation peut varier d'un pays à l'autre, y compris au sein de l'UE. Toutefois, comme nous l'avons souligné à l'Annexe 2, un niveau de coopération plus élevé avec le CEPD et des garanties plus élevées en matière de protection des données sont attendus pour les pays de l'UE, contrairement aux pays tiers.

- ***C3 - La multiplicité intrinsèque des utilisateurs des services publics en nuage,*** *qui hébergent généralement des données de différents clients dans le même centre de données, voire au sein du même périmètre de sécurité ou du même serveur***.**
  - **R6 - Des vulnérabilités possibles dans les politiques d'accès et les contrôles de sécurité**, comme des accidents et des attaques informatiques provenant de l'infrastructure client d'un ou de plusieurs utilisateurs du fournisseur de services en nuage, pourraient compromettre les données de l'institution de l'UE. En outre, les différents utilisateurs du fournisseur de services en nuage pourraient être établis dans des pays disposant d'un niveau de protection différent (inférieur) à l'égard des données à caractère personnel que celui des pays de l'UE (voir également R7).
- ***C4 - La localisation physique des données de l'utilisateur du nuage peut être inconnue de celui-ci ou, dans le cas contraire, rarement vérifiable.*** *Les fournisseurs de services en nuage de taille moyenne et de grande taille disposent généralement de centres de données dans de nombreux pays. Les données peuvent être situées de manière dynamique dans les différents centres de données en fonction de la disponibilité des ressources informatiques, des besoins de redondance et des facteurs économiques. La localisation des données n'est pas toujours communiquée à l'utilisateur du nuage ou, dans le cas contraire, elle l'est, mais avec peu de précision (par exemple, uniquement le nom du pays).*
  - Problèmes liés aux juridictions étrangères:
    - **R7 - Différentes législations applicables** et donc différents niveaux de protection des données possibles, selon principalement que les données sont situées au sein ou en dehors de l'UE. Il est également possible que le siège du fournisseur de services en nuage se situe dans l'UE, mais que l'entreprise possède des filiales ou des sous-traitants ultérieurs hors de l'UE. Différentes exigences, établies actuellement dans le règlement (CE) nº 45/2001 et, à l'avenir, dans la proposition de

règlement[65], s'appliquent dans ce cas à l'institution de l'UE, ce qui entraîne l'application des règles relatives aux transferts des données à caractère personnel à des pays tiers.

- **R8** - Risque accru que les **fournisseurs de services en nuage soient tenus de coopérer avec les autorités répressives ou de divulguer des données à ces dernières sur la base de règles différentes de celles de l'UE** ou, en tout état de cause, contraires aux règles applicables aux institutions de l'UE.

➢ **R9** - Risque accru pour **les utilisateurs du nuage et les personnes concernées de ne pas avoir le contrôle de leurs données** (localisation).

- ***C5 - Tendance à la «marchandisation» des services de TI.***

Les services en nuage offrent aux institutions de l'UE la possibilité de déléguer (plus ou moins, en fonction des modèles de service et de déploiement) la gestion des TI au fournisseur de services en nuage, souvent avec une interaction minimale pour la configuration et la fourniture du service.

Étant donné la nécessité de gérer une masse critique de ressources informatiques pour offrir des services en nuage et de la concentration des fournisseurs de services en nuage sur le marché, un déséquilibre contractuel existe souvent entre ces fournisseurs et les clients du nuage, en particulier si ces derniers sont des personnes ou des PME. Dans le contexte des institutions de l'UE, cela peut se produire en particulier avec les petites unités organisationnelles ainsi qu'avec les petites institutions et les petits organes.

Les économies d'échelle, qui permettent d'avoir des frais de service inférieurs, s'appuient également sur des modalités contractuelles rigides et une faible adaptation des caractéristiques et des conditions.

➢ **R10 - Contrats de service et conditions d'utilisation injustes et rigides**. D'éventuelles conditions d'utilisation et termes contractuels «à prendre ou à laisser» sont proposés laissant peu ou pas de place à la négociation et la possibilité que le fournisseur de services en nuage apporte des modifications aux termes du contrat de manière unilatérale, sans préavis ou alors très court. Il est possible que ces contrats n'offrent pas à l'institution de l'UE les instruments permettant de protéger les données à caractère personnel de manière adéquate et de respecter le règlement (CE)º 45/2001 et encore moins la proposition de règlement.

➢ **R9 - Risque accru pour les utilisateurs du nuage et les personnes concernées de ne pas avoir le contrôle de leurs données** (général). Ce risque n'est pas nouveau et est typique de l'externalisation, mais il est particulièrement important dans le cas des services en nuage. Malgré le niveau de délégation dont jouit le fournisseur de services en nuage, la responsabilité en tant que «responsable du traitement» de respecter les dispositions en matière de protection des données relève toujours de l'institution de l'UE.

➢ **R11 - Manque de contrôle des mesures de sécurité.** Les institutions de l'UE peuvent concevoir et mettre en œuvre des mesures de sécurité afin de protéger les données à caractère personnel pour la partie du service en nuage qu'ils contrôlent. Cela dépend grandement des modèles de service et de déploiement (voir les sections suivantes). Pour ce qui est délégué au fournisseur de services en nuage, les utilisateurs n'ont généralement pas la possibilité de maîtriser les risques liés à

[65] Voir l'article 9 du règlement et les articles 44 à 50 du RGPD.

la sécurité ni de choisir les contrôles de sécurité organisationnels et techniques appropriés, comme l'exige le règlement (CE) nº 45/2001[66] ainsi que la proposition de règlement[67].

- **R12 - Absence de contrôle** par l'utilisateur du nuage ou des tiers pour avoir l'assurance que le fournisseur de services en nuage, en tant que sous-traitant, agit pour le compte de l'institution de l'UE et fournit des garanties suffisantes concernant la mise en œuvre des contrôles de sécurité[68]; cela inclut également **des obstacles possibles aux activités de contrôle et d'enquête** par des autorités compétentes, y compris scientifiques.
- **R13 - Défis concernant les réponses efficaces aux personnes concernées exerçant leurs droits**, comme des demandes d'informations exhaustives sur le traitement des données à caractère personnel les concernant, des demandes de verrouillage et de suppression de données, etc., conformément au règlement (CE) nº 45/2001[69] et à la proposition de règlement[70].
- **R14 - «Enfermement propriétaire éventuel» à la suite de la vente ou de l'arrêt de l'activité du fournisseur de services en nuage**, en raison d'une faillite ou d'un autre événement inattendu: les données pourraient être indisponibles ou des dispositions contractuelles ou une législation différente en matière de protection des données pourraient s'appliquer pour le nouveau fournisseur de services en nuage sans que l'institution de l'UE soit en mesure d'intervenir.
- **R15 - Manque de portabilité des données.** Des formats propriétaires, des programmes de données spécifiques et l'utilisation d'autres applications de prise en charge pourraient mettre en péril la restitution efficace et effective des données et la configuration des machines virtuelles de l'institution de l'UE ou leur remise au nouveau fournisseur de services en nuage. En outre, il existe un risque que les données à caractère personnel ne soient pas effacées de manière définitive par le fournisseur de services en nuage (précédent) après la remise.

- ***C6 - Plusieurs fournisseurs et sous-traitants ultérieurs peuvent travailler ensemble, par exemple dans le cadre d'une approche complexe à plusieurs niveaux, en vue de fournir le service demandé, et l'intégration dynamique de nouveaux acteurs est souvent possible.***
  - **R16 - Répartition peu claire des responsabilités au sein de la chaîne des fournisseurs de services (fournisseur de services en nuage et sous-traitants ultérieurs)** dans la mise en œuvre des garanties et des exigences en matière de traitement des données à caractère personnel, comme la qualité et la sécurité des données, garantissant les droits des personnes concernées et la possibilité de procéder à des audits. Les responsabilités des sous-traitants et des sous-traitants ultérieurs pourraient se perdre au sein de la chaîne et elles ne seraient finalement assumées par personne.

[66] Articles 22, 35 et 36 du règlement.

[67] Article 32 à 34 du RGPD.

[68] Comme l'exige l'article 23 du règlement.

[69] Comme l'exige l'article 28 du RGPD.

[70] Voir les articles 13 à 20 du règlement et les articles 17 à 23 du RGPD.

- ***C7 - Nombre accru de transferts de données à caractère personnel réalisés de manière fluide et rapide, associant de nombreuses parties et traversant des frontières, et copies de données pour une meilleure disponibilité et un accès plus rapide.***

  - **R9 - Risque accru pour les utilisateurs du nuage et les personnes concernées de ne pas avoir le contrôle de leurs données** (localisation, compétence, niveau de protection).

  - **R13 - Défis possibles pour une application efficace des droits des personnes concernées** (voir ci-dessus).

  - **R17 - Défis concernant la conservation des données et la suppression effective des données**. Les applications disponibles fondées sur le nuage peuvent ne pas fournir des caractéristiques adéquates pour gérer correctement la période de conservation de sorte que les données soient supprimées de manière définitive lorsqu'elles ne sont plus nécessaires aux objectifs licitement poursuivis. En outre, le fournisseur de services en nuage pourrait utiliser une infrastructure en nuage dans laquelle les données peuvent être reproduites pour des permutations à chaud et pour récupération après sinistre avec le risque de garder des copies des données également après leur suppression via les fonctionnalités du service en nuage disponible. Des répertoires pourraient également être déplacés d'un serveur à un autre pour l'optimisation de l'infrastructure en nuage et une éventuelle défaillance du mécanisme laisserait des copies non nécessaires des données.

- ***C8 - La sécurité des données (à caractère personnel) dans une infrastructure en nuage comporte des risques spécifiques par rapport à un centre de données «traditionnel» local.***

  Si, dans certains cas, le fournisseur de services en nuage pourrait offrir de meilleures mesures de sécurité que celles mises en œuvre dans un centre de données «traditionnel» géré par l'institution de l'UE, la conception typique fondée sur le nuage introduit des risques spécifiques ou amplifie les risques existants.

  Certains problèmes de sécurité du nuage ayant des conséquences pour la protection des données ont déjà été recensés dans la présente section. Il convient de répondre également à d'autres risques spécifiques à la sécurité des TI.

  - **R18 - Autres risques liés à la sécurité des TI spécifiques à l'informatique en nuage (non exhaustifs):**

    - sécurité de l'agent de l'utilisateur (par exemple le navigateur, l'application mobile);
    - authenticité des services demandés;
    - gestion complexe des clés de chiffrement;
    - défis en matière d'identité et de gestion de l'authentification;
    - niveau de virtualisation et vulnérabilités des machines virtuelles.

Problèmes spécifiques dans le modèle de service IaaS

Dans ce modèle, les machines virtuelles sont attribuées par le fournisseur de services en nuage à l'utilisateur à partir d'une mise en commun des ressources partagées. L'utilisateur du nuage a le contrôle de nombreux aspects de la configuration de l'infrastructure de TI, de la plateforme logicielle et des applications développées sur celle-ci, mais il n'a aucun contrôle sur la sécurité physique du centre de données.

- ***C5***
    - Manque de transparence concernant certains aspects de l'infrastructure technique sous-jacente (logiciel de virtualisation de base, matériel et certains réseaux) et des garanties techniques et organisationnelles pertinentes.
    - Contrôle sur les mesures de sécurité au niveau de l'application et de la plateforme. Contrôle limité sur la sécurité de faible niveau de certaines machines logicielles, sur la sécurité des réseaux et absence de contrôle sur la sécurité physique des centres de données.
    - Exercice possible d'un contrôle au niveau de l'application, de la plateforme et de la configuration de la machine. Exercice limité (dans la mesure où le réseau est configurable) ou inexistant d'un contrôle au niveau du réseau et aucune maîtrise des caractéristiques du contrôle possible de la sécurité physique.
    - Possibilité de développer des outils visant à tenir compte des droits des personnes concernées.
    - Risques plus faibles liés à la portabilité.
- ***C3***
    - Ici, le risque est axé sur les ressources partagées (sécurité de l'infrastructure de réseau de base, sécurité physique et du matériel) et est inférieur par rapport aux modèles SaaS et PaaS.

Problèmes spécifiques dans le modèle de service PaaS

Dans ce modèle de service, les systèmes d'exploitation dotés de langages de programmation et d'autres outils logiciels comprenant des répertoires de données compatibles sont fournis par le fournisseur de services en nuage à l'utilisateur, déployés à l'aide de machines virtuelles. L'utilisateur du nuage n'a le contrôle que de certains aspects de la configuration de la plateforme, des applications développées sur la plateforme et des données traitées. Absence totale de contrôle sur l'infrastructure de TI sous-jacente et sur la sécurité physique du centre de données.

- ***C5***
    - Manque de transparence concernant certains aspects de l'infrastructure technique sous-jacente (sauf pour la configuration de la plateforme logicielle et des applications, du matériel et des réseaux) et des garanties techniques et organisationnelles pertinentes.
    - Contrôle sur les mesures de sécurité au niveau de l'application et contrôle modéré sur la plateforme. Contrôle limité sur la sécurité des réseaux et absence de contrôle sur la sécurité physique des centres de données.
    - Exercice possible d'un contrôle au niveau de l'application et de la plateforme. Exercice limité ou inexistant d'un contrôle au niveau du réseau et aucune maîtrise des audits possibles de la sécurité physique.
    - Possibilité de développer des outils visant à tenir compte des droits des personnes concernées.
    - Quelque défis en matière de portabilité en raison de divergences éventuelles dans l'exécution des plateformes logicielles et de problèmes éventuels de performance différents.
- ***C3***
    - Outre ce qui a déjà été mentionné, ici, les opérations de traitement appartenant à différents utilisateurs pourraient même partager le même serveur.

Problèmes spécifiques dans le modèle de service SaaS

L'utilisateur reçoit une application logicielle pour prendre en charge des processus d'activité spécifiques. L'utilisateur du nuage n'a le contrôle que sur la configuration de l'application fondée sur le nuage et sur les données traitées. Absence totale de contrôle sur le code de l'application des systèmes d'exploitation, les bases de données, les serveurs web, les serveurs d'application, les machines virtuelles et les logiciels de virtualisation de base, les serveurs physiques, les réseaux et les dispositifs de sécurité, la sécurité physique du centre de données.

- ***C1***
  - La probabilité de sous-estimer les risques ou de choisir des garanties inappropriées est plus élevée car les départements commerciaux pourraient être tentés d'acheter des services en nuage SaaS sans disposer de conseils d'experts suffisants en matière de protection des données et de TI.
- ***C5***
  - Manque de transparence et de contrôle sur le code de l'application et sur l'infrastructure technique sous-jacente ainsi que sur les garanties techniques et organisationnelles.
  - Absence de contrôle sur les mesures de sécurité, mais contrôle modéré au niveau de l'application (par exemple l'authentification et l'autorisation par l'utilisateur des caractéristiques de l'application).
  - Absence de contrôle particulièrement criante.
  - Manque éventuel d'outils permettant de tenir compte des droits des personnes concernées.
  - Le manque de portabilité pourrait être accru par des formats spécifiques et d'autres contraintes possibles, comme l'application de règles d'entreprises, des flux de travail spécifiques, le contexte et la dépendance à d'autres applications.
- ***C3***
  - Outre les éléments déjà mentionnés, il s'agit ici plus particulièrement, par exemple, des opérations de traitement appartenant à différents utilisateurs pouvant fonctionner sur la même machine virtuelle ,voire dans la même instance d'application, ce qui accroît davantage les risques.

Problèmes spécifiques dans le modèle de déploiement en nuage privé/communautaire externalisé

Ici, certaines machines au sein d'un périmètre de sécurité spécifique à un/des utilisateur(s) sont déployées dans les centres de données du fournisseur de services en nuage à l'usage exclusif de/des utilisateur(s) du nuage.

- ***C2***

  Les services ne sont pas nécessairement offerts par l'internet public: si c'est le cas, pas de risques importants.

  Un moyen de communication dédié pourrait être disponible ou mis en place. Dans ce cas:
  - Risques possibles liés à la confidentialité et à l'intégrité limités au fournisseur de service de communication.
  - Manque de disponibilité liée à l'indisponibilité du fournisseur de service de communication (en raison d'une défaillance technique ou autre).

- Risques possibles liés à la conservation des données à des fins d'application de la législation.

- ***C3***
  - Le risque est moins élevé (même celui de l'IaaS public) et souvent limité à la sécurité physique et à certaines ressources de réseau de base. Toutefois, les systèmes précédemment déployés dans différents périmètres de sécurité et sous différentes responsabilités sont désormais réunis dans la même infrastructure en nuage et exposés à des risques liés à la sécurité différents. Cela s'applique d'autant plus aux nuages communautaires.

- ***C4***
  - Ce risque est beaucoup moins élevé ou, plus souvent, n'existe pas dans un nuage privé externalisé.

- ***C5***
  - Les risques liés à la transparence, au choix des mesures de sécurité et au contrôle sont beaucoup moins élevés, puisqu'en général l'utilisateur dispose d'un plus grand contrôle.
  - Risque beaucoup moins élevé de ne pas tenir compte des droits des personnes concernées, ayant un niveau de contrôle qui est généralement plus élevé que dans l'IaaS public.
  - Risques liés à la portabilité plus faibles.

- ***C6***
  - En présence de contractants externes, le risque est toujours présent, bien qu'il soit généralement plus faible que dans les nuages publics, car l'utilisateur a un plus grand pouvoir de négociation contractuelle.

- ***C7***

Les localisations sont généralement connues de l'utilisateur et le traitement est soumis à un plus grand contrôle:

- Risques beaucoup moins élevés liés aux transferts des droits des personnes concernées.
- Risques moins élevés pour la conservation des données et la suppression effective, simplement en raison des mécanismes intrinsèques fluides d'attribution des ressources dans une infrastructure fondée sur le nuage (redondance, attribution dynamique, paradigme réparti).

- ***C8***
  - Le risque suivant est très limité si l'internet public n'est pas utilisé comme moyen de communication avec les services externalisés:
    - authenticité des services demandés
  - Les risques suivants sont en général très limités:
    - gestion complexe des clés de chiffrement
    - défis en matière d'identité et de gestion de l'authentification

Problèmes spécifiques dans le modèle de déploiement en nuage privé/communautaire sur site

Ici, l'infrastructure en nuage est déployée au sein du périmètre de sécurité de/des utilisateur(s) dans ses/leurs locaux. En cas de nuages communautaires, une ou plusieurs entités participantes hébergeront l'infrastructure pour toutes.

- ***C2***
  - Les services ne sont pas offerts via l'internet public: aucun risque important pour les nuages privés. En cas de nuages communautaires, certains utilisateurs du nuage devront utiliser des dispositifs de communication pour établir le contact. Dans ce cas, les mêmes considérations que pour les nuages communautaires externalisés s'appliquent.
- ***C3***
  - Principalement un risque beaucoup moins élevé. Toutefois, les systèmes précédemment déployés dans différents périmètres de sécurité et sous différentes responsabilités sont désormais réunis dans la même infrastructure en nuage et sont donc exposés à des risques différents concernant la sécurité. Cela s'applique d'autant plus aux nuages communautaires.
- ***C4***

La localisation physique des données de l'utilisateur du nuage est connue de l'utilisateur: pas de risques importants.

- ***C5***

  En général, risque très faible ou absent, mais:
  - Il subsiste certains risques très faibles liés à la transparence en raison de mécanismes intrinsèques fluides d'attribution des ressources dans une infrastructure fondée sur le nuage. Toutefois, l'utilisateur en a le contrôle intégral.
  - Certains risques très faibles subsistent pour l'application effective des droits des personnes concernées en raison des mécanismes intrinsèques fluides d'attribution des ressources dans une infrastructure fondée sur le nuage (redondance, attribution dynamique, paradigme réparti). Toutefois, l'utilisateur en a le contrôle intégral.
- ***C6***
  - Aucun risque de répartition peu claire des responsabilités si l'infrastructure en nuage est gérée par le personnel interne.
- ***C7***

  Les localisations sont connues de l'utilisateur et le traitement est soumis à un plus grand contrôle:
  - Risques beaucoup moins élevés ou absents liés aux transferts des droits des personnes concernées.
  - Certains risques très faibles subsistent pour la conservation des données et la suppression effective, simplement en raison des mécanismes intrinsèques fluides d'attribution des ressources dans une infrastructure fondée sur le nuage (redondance, attribution dynamique, paradigme réparti).

- ***C8***
    - Les risques suivants sont beaucoup moins élevés ou disparaissent étant donné que l'infrastructure en nuage est privée et non externalisée:
        - gestion complexe des clés de chiffrement
        - défis en matière d'identité et de gestion de l'authentification
        - authenticité des services demandés

Annexe 5. Références et conseils de lecture

Documents stratégiques du groupe de travail «article 29» du CEPD

- Avis du contrôleur européen de la protection des données relatif à la communication de la Commission intitulée «Exploiter le potentiel de l'informatique en nuage en Europe», novembre 2012:

  https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_FR.pdf

- Avis 05/2012 du groupe de travail «article 29» sur l'informatique en nuage:

  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_fr.pdf

Documents stratégiques d'autres autorités chargées de la protection des données dans l'UE

- «Guidance on the use of cloud computing» - UK Information Commissioner's Office (ICO), octobre 2012:

  https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

- «Personal data protection and cloud computing» - Information Commissioner of Slovenia, juin 2012:

  https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Cloud_computing_and_data_protection_-_ENG_final.pdf

- «Data protection 'in the cloud'» - Data Protection Commissioner of Ireland, juillet 2012:

  https://www.dataprotection.ie/docs/03/07/12_Cloud_Computing/1221.htm

- Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing - Commission nationale de l'informatique et des libertés (France), juin 2012:

  https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

- «Cloud computing: how to protect your data without falling from a cloud» - Vademecum - Garante per la Protezione dei Dati Personali:

  http://194.242.234.211/documents/10160/2052659/CLOUD+COMPUTING+%E2%80%93+PROTECT+YOUR+DATA+WITHOUT+FALLING+FROM+A+CLOUD.pdf

- Guía para clientes que contraten servicios de Cloud Computing - 2013, Agencia Española de Protección de Datos:

  http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

- Resolution on cloud computing, Punta del Este, Uruguay, 26 octobre 2012, 34° Conferencia Internacional de Autoridades de protección dos datos y privacidad:

  http://194.242.234.211/documents/10160/2150357/Resolution+on+Cloud+Computing.pdf

Documents et références de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA)

- Sur l'informatique en nuage: https://www.enisa.europa.eu/topics/cloud-and-big-data

Voir en particulier:

- Publications pertinentes: https://www.enisa.europa.eu/topics/cloud-and-big-data?tab=publications
- Articles pertinents: https://www.enisa.europa.eu/topics/cloud-and-big-data?tab=articles
- Sur la sécurité en nuage: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

Documents d'organismes de normalisation

- «Privacy in Cloud Computing» - International Telecommunication Union Telecommunication Standardisation Sector (ITU-T) Watch Report, mars 2012:

  http://www.itu.int/en/ITU-T/techwatch/Pages/cloud-computing-privacy.aspx

- ISO/IEC 27017:2015 - Technologies de l'information -- Techniques de sécurité -- Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage:

  https://www.iso.org/standard/43757.html

- ISO/IEC 27018:2014 - Technologies de l'information -- Techniques de sécurité -- Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII:

  http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

Documents du secteur: Cloud Select Industry Group (CSIG)

- «Cloud Service Level Agreement Standardisation Guidelines» - Cloud Select Industry Group - Bruxelles, 24 juin 2014:

  https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

Documents du secteur: Cloud Security Alliance (CSA)

https://cloudsecurityalliance.org/download/

Documents stratégiques du groupe de travail international sur la protection des données dans les télécommunications (groupe de Berlin)

- Working Paper on Cloud Computing - Privacy and data protection issues - «Protocole d'accord de Sopot», groupe de Berlin, avril 2012:

  https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=3065

Documents techniques du NIST

- NIST Cloud Computing Program

  https://www.nist.gov/programs-projects/cloud-computing

- «The NIST Definition of Cloud Computing» - NIST Special Publication 800-145, septembre 2011:

  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- «Cloud Computing Synopsis and Recommendations» - NIST Special Publication 800-146, mai 2012:

  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

- «Guidelines on Security and Privacy in Public Cloud Computing» - NIST Special Publication 800-144, décembre 2011:

  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Autres documents stratégiques et techniques

- «Cloud Computing Security Considerations» - Australian Government Department of Defence - Intelligence and Security - Cyber Security Operations Centre, septembre 2012:

  http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf