EUROPEAN DATA PROTECTION SUPERVISOR

Lignes directrices sur la protection des données à caractère personnel dans les dispositifs mobiles utilisés par les institutions européennes

Décembre 2015

TABLE DES MATIÈRES

SYNTHÈSE

La popularité des dispositifs mobiles tient à la commodité, et à la grande fonctionnalité, qu'ils offrent à leurs utilisateurs, en complément de l'utilisation fonctionnelle des ressources informatiques. Pour autant, leur utilisation comporte des risques spécifiques liés à la protection des données, en raison de la portabilité de ces dispositifs et de la destination d'un grand nombre d'entre eux à un usage par les consommateurs, plutôt qu'à un usage professionnel.

Les présentes lignes directrices ont pour but de fournir aux institutions et organes de l'Union européenne des conseils et instructions concernant les données à caractère personnel et l'utilisation de dispositifs mobiles à des fins professionnelles, pour s'assurer qu'ils respectent leurs obligations telles qu'énoncées dans le règlement (CE) nº 45/2001 sur la protection des données applicables aux institutions européennes (le «règlement»).

S'ils sont activement associés, dès le début, à la planification de l'introduction de l'utilisation de dispositifs mobiles, le délégué à la protection des données et les coordinateurs de la protection des données ou contacts, le cas échéant, pourront donner des conseils, suggérer des améliorations et aider de manière générale l'institution à veiller au respect du règlement.

Les institutions européennes doivent mettre en balance les avantages d'une utilisation de dispositifs mobiles dans chaque opération (au cas par cas) et les risques et le caractère intrusif éventuellement associés à cette utilisation. Cette appréciation devrait également tenir compte des fonctionnalités et caractéristiques supplémentaires des dispositifs mobiles et des conséquences de l'introduction de tels dispositifs sur la sécurité de l'infrastructure informatique.

Une politique d'utilisation acceptable des dispositifs mobiles est essentielle pour régler la relation entre les institutions européennes et leur personnel. Lorsque la pratique du «Bring your own device» (BYOD) est permise, cette politique d'utilisation est d'autant plus importante que les droits et obligations des institutions européennes et de leur personnel doivent être précisés lorsque des équipements personnels sont utilisés à des fins professionnelles.

Cette pratique du BYOD gagne en popularité, puisque les avantages liés aux dispositifs mobiles offrent une plus grande flexibilité aux institutions et à leur personnel dans la manière de travailler. D'autre part, ces dispositifs comportent également des risques spécifiques pour les données des entreprises et des particuliers, qu'il convient d'examiner avant toute introduction. Une politique spéciale de BYOD sera également requise.

La sécurité est l'un des grands instruments de la protection des données. Pour garantir un niveau adéquat de protection, les institutions européennes doivent engager un processus de gestion des risques permettant d'apprécier les risques pour la sécurité liés à une utilisation de dispositifs mobiles dans le cadre du traitement des données à caractère personnel; les institutions doivent ensuite appliquer des mesures pour faire face aux risques détectés. Ces mesures relèvent à la fois de l'organisation, comme l'adoption de politiques de sécurité de l'information, et du domaine technique, comme les solutions de gestion des dispositifs mobiles.

Pour contrôler comme il se doit les dispositifs mobiles, qu'ils appartiennent aux institutions européennes ou qu'ils soient personnels, les institutions devraient adopter des procédures écrites afin de gérer le cycle de vie de ces dispositifs. Ces procédures devraient tenir compte de toutes les opérations qui doivent être exécutées avec le dispositif.

Les mesures précitées devraient refléter les politiques adoptées par les institutions européennes et être imaginées selon les principes de «l'intégration des principes de protection des données dès la phase de conception» et de «protection de la vie privée par défaut». Elles ne devraient pas collecter ni traiter plus de données à caractère personnel qu'il n'en faut (principe de la minimisation des données).

Les présentes lignes directrices abordent les aspects sécuritaires, tels qu'énoncés dans le règlement, du traitement des données à caractère personnel par les institutions européennes à l'aide de dispositifs mobiles. Nous recommandons de lire ce document conjointement avec les lignes directrices du CEPD sur les données à caractère personnel et les communications électroniques au sein des institutions de

l'Union, qui abordent également la question du contrôle des dispositifs mobiles par les institutions européennes.

Si les présentes lignes directrices sont en principe destinées aux institutions européennes, elles peuvent également être utiles à toute personne ou organisation intéressée par la protection des données et les dispositifs mobiles; par de nombreux aspects, le règlement (CE) nº 45/2001 est similaire à la directive 95/46/CE relative à la protection des données, transposée dans les législations nationales des États membres de l'UE, ainsi qu'aux règles nationales en Islande, au Liechtenstein et en Norvège.

I. Introduction

I.1. Les lignes directrices

1 Lorsque les membres du personnel des institutions, organes ou agences de l'UE (les «institutions européennes») utilisent des dispositifs mobiles dans le cadre de leurs besoins opérationnels, il arrive qu'ils traitent sur ces dispositifs des données à caractère personnel de tiers. Ce constat pourrait s'appliquer à toute personne en contact avec les institutions européennes: un citoyen qui utilise l'un des services de l'UE, un membre du personnel, un contractant, une personne qui demande un financement de l'UE, un membre de la presse ou autre. Dans ces situations, il incombe à l'institution d'assurer le respect des principes de protection des données, en particulier du règlement (CE) nº 45/2001[1] (le «règlement»), afin de garantir les droits au respect de la vie privée et à la protection des données à caractère personnel. Cette responsabilité revient à l'institution européenne concernée, quelle que soit l'origine des dispositifs mobiles, qu'ils soient fournis par les institutions européennes aux membres de l'encadrement et au personnel ayant des besoins professionnels particuliers, ou qu'il s'agisse de **dispositifs personnels** que le personnel est autorisé à utiliser à des fins professionnelles («Bring Your Own Device», BYOD).

2 En tant qu'autorité de contrôle indépendante compétente pour le traitement des données à caractère personnel par les institutions européennes, le Contrôleur européen de la protection des données (CEPD) peut, entre autres tâches, publier des lignes directrices sur des questions précisément liées au traitement des données à caractère personnel[2]. Les présentes lignes directrices sont **le résultat d'un processus** au cours duquel les institutions européennes ont été consultées.

3 Les 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, ainsi qu'au personnel du service informatique et de la sécurité informatique et aux autres services administratifs concernés par les procédures qui gravitent autour de l'utilisation professionnelle de dispositifs mobiles et, enfin, à toutes les personnes qui ont la responsabilité d'agir en tant que responsables du traitement au sein des institutions européennes.

4 Les lignes directrices fournissent une analyse des risques génériques pour la protection des données dans le cadre du traitement de données à caractère personnel sur des dispositifs mobiles ainsi que des recommandations et des bonnes pratiques qui devraient aider les institutions européennes à atteindre un niveau de protection des données conforme au règlement. Si ces lignes directrices ont pour objet d'aider les institutions européennes à remplir plus facilement leurs obligations, elles ne déchargent pas les institutions européennes qui les appliquent de leurs responsabilités.

[1] 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).

[2] Dans l'exercice des pouvoirs qui lui sont conférés à l'article 41, paragraphe 2, et à l'article 46, point d), du règlement.

Les institutions européennes restent tenues d'apprécier et d'atténuer comme il se doit les risques liés au traitement. La liste d'actions et de mesures recommandées dans les présentes lignes directrices ne se veut ni exhaustive ni exclusive. Le CEPD considèrera les bonnes pratiques énoncées ci-après comme un «critère» pour évaluer la conformité, mais les institutions européennes sont encouragées à réaliser leur propre analyse de risque et à choisir les mesures adéquates en conséquence. Elles peuvent opter pour des mesures différentes de celles contenues dans le présent document; le CEPD évaluera les mesures mises en place au sein d'une institution européenne selon des critères d'exhaustivité et d'efficacité, et non en fonction de la conformité aux présentes lignes directrices.

I.2. Contexte technique

5 Les dispositifs mobiles, essentiellement les smartphones et tablettes, envahissent nos vies professionnelles et privées. Il s'agit désormais de «dispositifs informatiques universels» qui prennent en charge pratiquement toutes les applications. En outre des appels vocaux et des messages textuels, ils offrent la possibilité d'utiliser les services de l'internet (réseaux sociaux, partage de contenu, etc.) et sont dotés de nombreux capteurs qui fournissent de plus en plus d'informations sur leurs utilisateurs, comme la localisation ainsi qu'un nombre croissant de paramètres environnementaux et personnels.

6 Les dispositifs mobiles intelligents ont **révolutionné** la manière dont les organisations travaillent. De plus en plus d'applications sont développées pour ces dispositifs et remplacent les postes de travail et les ordinateurs portables pour certaines tâches. Leur utilité tient à la satisfaction grandissante qu'ils procurent aux travailleurs et aux économies de coûts qu'ils permettent; en outre, ils présentent l'avantage de se prêter au besoin de mobilité croissant.

7 **Les smartphones et tablettes ne sont pas les seuls dispositifs mobiles** utilisés dans les organisations: les dispositifs de stockage portables, comme les cartes à mémoire, les clés USB et les lecteurs de disques durs ont également repoussé les limites du stockage, de la transmission et de la sécurité des données. Les **risques pour la sécurité et la vie privée** liés à leur utilisation sont importants et ne sauraient être négligés.

8 À cet égard, plusieurs **points critiques** ont été recensés:

- les utilisateurs de dispositifs mobiles dans le cadre professionnel des institutions européennes traitent souvent des données à caractère personnel **sans savoir** qu'une action sur le dispositif mobile peut impliquer un traitement de données à caractère personnel soumis aux conditions et aux limites du règlement. Il arrive que les institutions européennes ne réalisent pas – puisque les opérations de traitement de données réalisées par leurs membres du personnel dans l'exercice de leurs fonctions sont imputables à l'institution européenne concernée – qu'elles restent responsables de ces opérations de traitement, même lorsque ces opérations

sont seulement «transactionnelles» (par exemple, transmettre un courrier électronique contenant les coordonnées d'un nouveau collègue);

- les dispositifs mobiles «**intelligents**» permettent d'utiliser des logiciels d'application qui interagissent avec des ressources en ligne. Ils échangent des informations à travers leur interface réseau, parfois sans que les utilisateurs ou les institutions le remarquent;
- lorsque le personnel des institutions européennes utilise ses propres dispositifs personnels à des fins professionnelles (par exemple, pour accéder à des informations informatiques ou pour les stocker), cela soulève de nouvelles questions liées à la protection des données. L'utilisateur se sert du même dispositif pour ses communications personnelles et à d'autres fins, à l'aide des applications qu'il a choisi d'installer. Les institutions européennes ne peuvent exercer le même niveau de vérification et de contrôle sur les dispositifs personnels qu'elles ne le font pour les dispositifs leur appartenant.

9 Le principe de **responsabilité** revêt une importance capitale dans le cadre de l'utilisation de dispositifs mobiles. C'est d'autant plus important qu'il est compliqué de définir clairement les responsabilités propres à chaque acteur concerné selon la multitude des utilisations possibles. Une **coopération étroite entre les délégués à la protection des données et les responsables de la sécurité de l'information** des institutions européennes est vivement recommandée.

II. Champ d'application, méthodologie et structure des lignes directrices

II.1. Champ d'application

10 Les présentes lignes directrices donnent des conseils pour respecter les règles relatives au respect de la vie privée et à la protection des données dans le cadre de l'utilisation de dispositifs mobiles par les membres du personnel des institutions européennes à des fins professionnelles. Ces conseils sont sans préjudice d'une politique distincte ou spécifique que les institutions européennes pourraient envisager d'appliquer à leurs représentants politiques ou de haut niveau.

11 Ces lignes directrices couvrent à la fois les dispositifs mobiles fournis par les institutions européennes et ceux appartenant à leur personnel, lorsqu'ils sont utilisés à des fins professionnelles (BYOD). Le terme «**dispositifs mobiles**» comprend les téléphones, les smartphones, les tablettes, les ordinateurs portables et les netbooks, autrement dit tous les dispositifs qui permettent au personnel de travailler en mobilité, ainsi que les dispositifs de stockage comme les lecteurs de disques durs externes et les clés USB. Ces dispositifs présentent des risques communs dus à leur nature «mobile» et à leur petite taille; pourtant les mesures de sécurité qui peuvent s'y appliquer seront différentes. Les présentes lignes directrices portent principalement sur les smartphones et les tablettes. Pour les autres dispositifs mobiles, des sous-ensembles de risques et les mesures recommandées s'appliquent.

12 Si l'utilisation de dispositifs mobiles à des fins professionnelles soulève généralement de nombreuses questions liées à la sécurité informatique, les risques concernant les informations détenues par les institutions européennes relèvent du champ d'application des présentes lignes directrices seulement dans la mesure où les risques informatiques ont une incidence sur les données à caractère personnel.

13 Les présentes lignes directrices abordent les **questions** suivantes:

- les **principes généraux** du traitement des données à caractère personnel au moyen de dispositifs mobiles par les institutions européennes;
- les **risques pour les données à caractère personnel** traitées sur des dispositifs mobiles;
- les **bonnes pratiques** pour protéger les données à caractère personnel.

14 Les présentes lignes directrices **n'abordent pas** les scénarios et thèmes suivants:

- le personnel utilise des **dispositifs appartenant aux institutions européennes**[3] **à des fins personnelles**;
- le personnel utilise des **dispositifs mobiles personnels uniquement à des fins personnelles** (même sur le lieu de travail);
- les risques pour les intérêts et les biens des institutions européennes, autres que ceux liés à la protection des données à caractère personnel (par exemple, la protection de la propriété intellectuelle ou d'informations classées «confidentielles»);
- le traitement de données sur les communications électroniques pour détecter un usage non autorisé de dispositifs mobiles[4]; et
- la criminalistique numérique sur les dispositifs mobiles des membres du personnel par les institutions européennes compétentes dans le cadre d'enquêtes[5].

II.2. Méthodologie

15 Le processus qui a présidé aux présentes lignes directrices a été conçu de telle manière qu'elles sont le résultat d'un **dialogue ouvert structuré** avec les institutions européennes. Les éléments/étapes clés de ce processus sont les suivants:

- l'enquête du 21 juin 2013 visant à constater des faits et à parvenir à une meilleure compréhension de la position des institutions européennes sur cette question;

[3] L'utilisation d'un dispositif mobile par un membre du personnel **à des fins personnelles** ne correspond pas à un traitement effectué par une institution européenne ou pour le compte de celle-ci. Par conséquent elle se situe **hors du champ d'application du règlement**.

[4] Ce point est couvert dans les lignes directrices sur les données à caractère personnel et les communications électroniques au sein des institutions de l'Union.

[5] Ibid.

- l'atelier du 19 septembre 2013 sur ce sujet, articulé autour d'un document d'orientation transmis au préalable aux participants, au cours duquel le CEPD a également présenté les résultats de l'enquête;
- l'examen des bonnes pratiques pour la sécurité des dispositifs mobiles;
- la transmission de la version préliminaire des lignes directrices aux institutions européennes pour avoir leur avis; et
- la prise en considération de cet avis pour établir la version finale des lignes directrices.

16 Le CEPD révisera régulièrement les présentes lignes directrices et continuera de faire appel aux institutions européennes dans le cadre d'un dialogue ouvert. Une première révision devrait avoir lieu deux ans après l'adoption.

II.3. Structure

17 Le présent document est structuré comme suit.

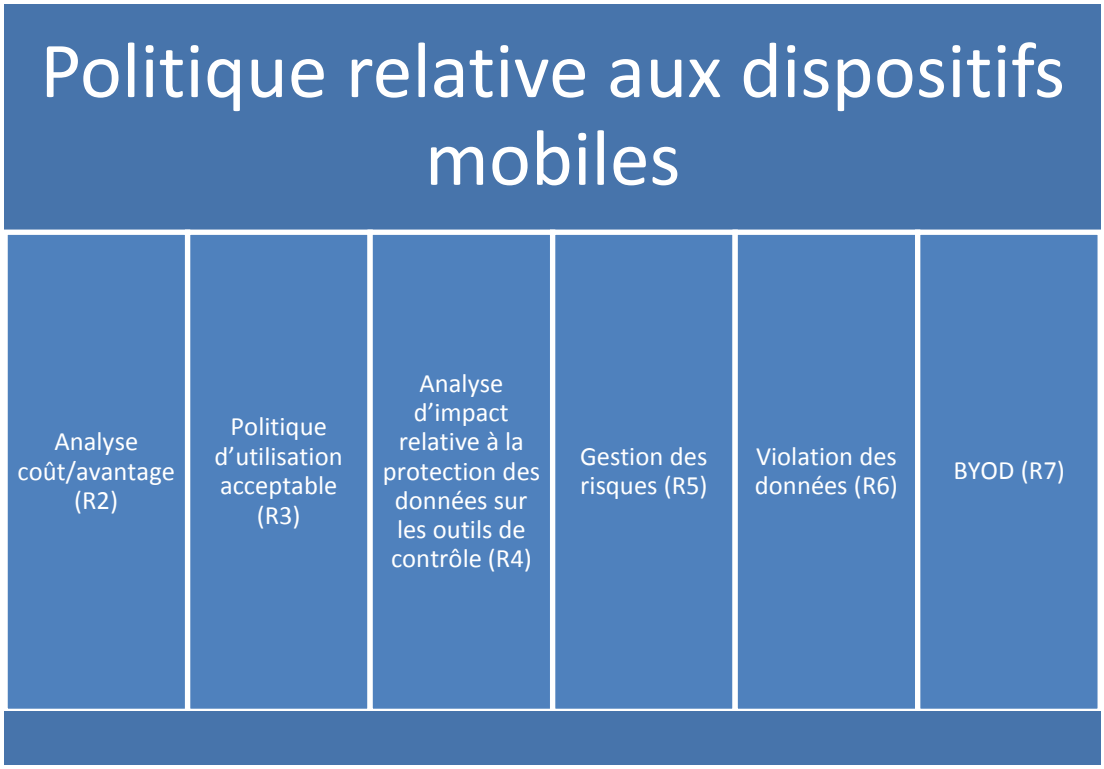
- La section III *Recommandations* présente la liste des recommandations à appliquer, sur la base des obligations énoncées dans le règlement. Le contenu de cette section est le plus pertinent pour les DPD/CPD et le personnel du service informatique/de la sécurité informatique des institutions européennes, car il indique ce qu'une «politique relative aux dispositifs mobiles» devrait prévoir.
- La section IV *Mesures de sécurité pour protéger les données à caractère personnel* traitées au moyen de dispositifs mobiles propose quelques mesures de sécurité inspirées des bonnes pratiques que les institutions européennes peuvent appliquer pour faire face aux risques liés aux dispositifs mobiles semblables à ceux présentés dans la section VI.
- La section V *Problèmes relatifs à la protection des données dans le cadre du traitement de* données à caractère personnel au moyen de dispositifs mobiles aborde plus en détail les différentes questions juridiques qui se posent dans l'utilisation des dispositifs mobiles relevant du champ d'application du présent document.
- La section VI *Risques pour les données à caractère personnel traitées* sur des dispositifs mobiles décrit certains risques liés aux dispositifs mobiles.

Le texte en italique dans un encadré apporte des exemples et des clarifications au contenu du texte qui précède.

Les sections répondent aux besoins des différentes parties prenantes qui interviennent dans la problématique des dispositifs mobiles: la section III devrait être consultée par tous, car elle décrit les obligations qui découlent du règlement. Les sections IV et VI contiennent les informations techniques les plus utiles des présentes lignes directrices sous la forme de mesures de sécurité et de risques liés à l'utilisation de dispositifs mobiles. Enfin, la section V analyse les cas particuliers du traitement de données à caractère personnel au moyen de dispositifs mobiles d'un point de vue juridique.

III. Recommandations

18 Cette section comprend un ensemble de recommandations visant à aider une institution européenne à établir qu'elle respecte le règlement lorsqu'elle traite des données à caractère personnel au moyen de dispositifs mobiles. Ces recommandations peuvent s'entendre comme les différents volets d'une *politique relative aux dispositifs mobiles*, à l'image du diagramme suivant.



R1: Associer le DPD dans tous les aspects de l'introduction et de l'utilisation de dispositifs mobiles au sein des institutions européennes. *(Voir section V.1)*

Il importe que le DPD participe à l'introduction de l'utilisation de dispositifs mobiles dès la planification, afin de veiller à ce que les mesures prises soient conformes au règlement.

R2: Réaliser une **évaluation au cas par cas des avantages d'une utilisation de dispositifs mobiles dans telle ou telle opération de traitement en tenant compte des risques et du caractère intrusif** éventuellement associés à cette utilisation. *(Voir section V.1).*

Cette appréciation devrait tenir compte des fonctionnalités et caractéristiques supplémentaires du dispositif mobile, par exemple la possibilité d'étoffer la liste des contacts en y ajoutant les photos des personnes prises à l'aide de l'appareil photo du dispositif mobile.

Elle devrait également tenir compte des conséquences de l'introduction de dispositifs mobiles sur la sécurité de l'infrastructure informatique actuelle. L'introduction de dispositifs mobiles non sécurisés risque de représenter une menace pour la sécurité d'une infrastructure informatique conçue sur l'idée que tous les dispositifs sont sécurisés et que les attaques sont lancées depuis l'extérieur du réseau. (Voir section V.2)

R3: Les institutions européennes concernées devraient adopter une **politique d'utilisation acceptable** des dispositifs mobiles *(voir section V.1*). Cette politique devrait également imposer des obligations aux utilisateurs concernant le cycle de vie des dispositifs mobiles.

R4: Une **analyse d'impact relative à la protection des données** devrait être réalisée sur les outils de surveillance et de contrôle utilisés pour garantir la sécurité des dispositifs mobiles. Cette analyse devrait passer en revue les grands principes et les conditions générales de la protection des données énoncés dans le règlement, notamment la licéité, la nécessité et la proportionnalité; la spécification et la limitation de la finalité; la qualité des données, la conservation des données; les informations sur les personnes concernées et leurs droits (accès, rectification, effacement, verrouillage); les transferts de données et la confidentialité des réseaux de télécommunications ou équipements de terminaux internes *(voir section V.3).*

Dès qu'une analyse d'impact relative à la protection des données est réalisée pour une opération de traitement, l'utilisation de dispositifs mobiles pour cette opération de traitement doit être prise en considération. Cette analyse d'impact pourrait être réalisée parallèlement à l'évaluation des risques pour la sécurité informatique et devrait, en tout état de cause, examiner les risques pour la sécurité qui s'y rapportent (voir section V.3).

R5: Disposer d'un **processus de gestion des risques** documenté de façon appropriée: les responsables du traitement doivent prendre les mesures techniques et organisationnelles appropriées afin de garantir la sécurité d'utilisation des dispositifs mobiles. Ces mesures devraient assurer un niveau de sécurité approprié au regard des risques présentés, compte tenu des solutions techniques disponibles et des coûts liés à leur mise en œuvre *(voir section V.2).*

La section VI Risques pour les données à caractère personnel traitées sur des dispositifs mobiles décrit certains risques liés aux dispositifs mobiles. Les institutions européennes devraient passer en revue ces risques lorsqu'elles réalisent leur évaluation des risques. En outre, la section IV, Mesures de sécurité pour protéger les données à caractère personnel traitées au moyen de dispositifs mobiles, recense certaines bonnes pratiques en matière de mesures de sécurité. Les institutions européennes devraient considérer ces mesures comme des moyens de contrer les risques qu'elles évalueront.

R6: Adopter en interne des **procédures pour gérer les violations de données**, notamment la notification par le responsable du traitement au DPD et au CEPD *(voir section V.4)*.

R7: Lorsque le **BYOD** est autorisé, toutes les institutions européennes concernées devraient:

- évaluer les risques pour les données à caractère personnel des institutions et des particuliers avant d'introduire le BYOD dans l'organisation *(voir section V.2)*;
- disposer d'une politique régissant le BYOD. *(Voir section V.1).*

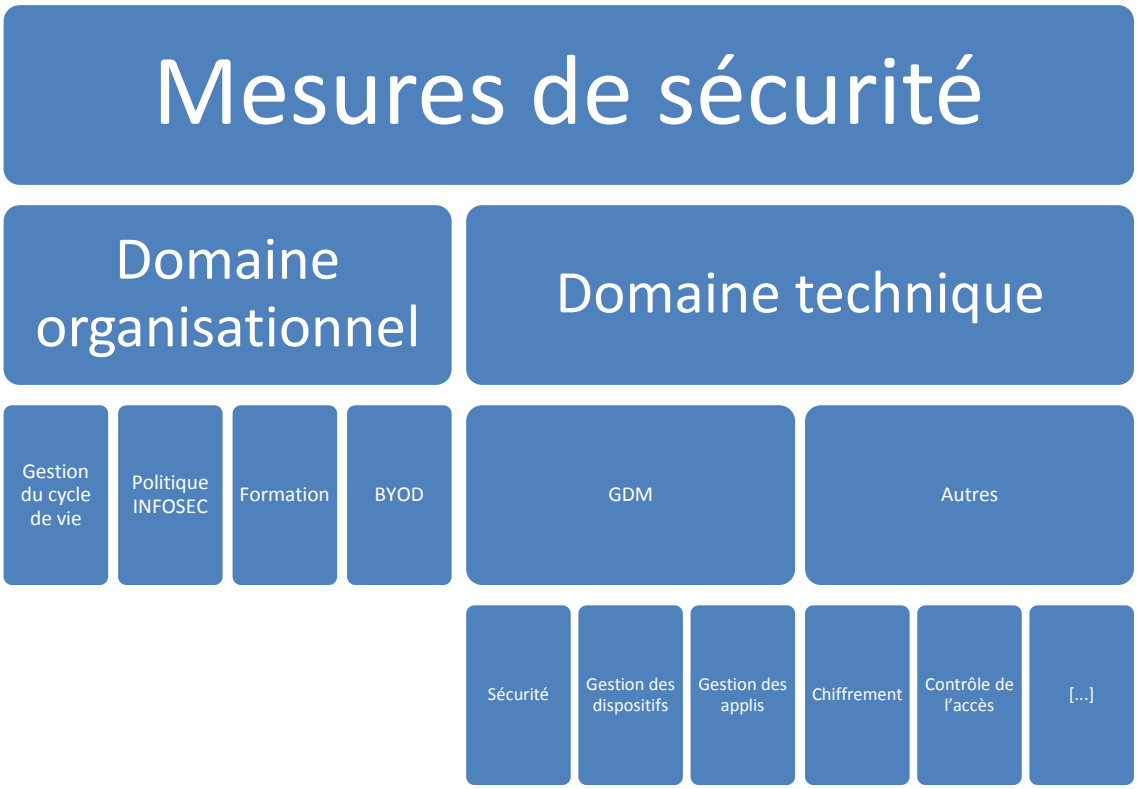
R8: S'il existe des copies locales de données à caractère personnel sur des dispositifs mobiles, il est également essentiel que les données à caractère personnel stockées sur le dispositif mobile fassent également l'objet d'une rectification, d'un verrouillage ou d'un effacement lorsque la personne concernée exerce son droit de rectification des données à caractère personnel inexactes ou incomplètes, ou le droit de verrouillage ou d'effacement de données traitées de manière illicite. *(Voir section V.5).*

R9: En principe, l'utilisation de dispositifs mobiles n'est pas, en tant que telle, une raison pour soumettre les opérations de traitement au contrôle préalable effectué par le CEPD en vertu de l'article 27 du règlement *(voir section V.1)*. La nécessité de soumettre une opération de traitement au contrôle préalable du CEPD doit être analysée au regard de la «finalité» du traitement, conformément à l'article 27, paragraphe 2, du règlement.

IV. Mesures de sécurité pour protéger les données à caractère personnel traitées au moyen de dispositifs mobiles

19 Cette section propose une liste de mesures de sécurité recommandées sur les plans technique et organisationnel. Cette liste n'est pas exhaustive et les institutions européennes sont libres de faire leur choix parmi les mesures proposées ou d'adopter d'autres mesures répondant à leurs besoins particuliers, en fonction de leur propre évaluation des risques et du niveau de sécurité requis.

Le diagramme suivant résume ces mesures de sécurité:



IV.1. Mesures organisationnelles

20 L'introduction de dispositifs mobiles au sein d'une organisation demande la mise en place d'une politique globale comprenant des processus, des plans de formation, la participation de l'encadrement, et des procédures en cas d'incidents tels que des violations de données.

IV.1.1. Gestion du cycle de vie d'un dispositif mobile

21 Les institutions européennes concernées devraient adopter des **procédures** documentées applicables à la gestion du cycle de vie complet des dispositifs mobiles.

22 Ces procédures devraient couvrir toutes les phases qui entrent en ligne de compte dans le cycle de vie du dispositif mobile, du moment où on l'achète au moment où on l'élimine, en tenant compte de toutes les opérations qui doivent être réalisées sur le dispositif.

23 Dans le cadre de la gestion du cycle de vie, les institutions européennes devront instaurer et tenir à jour un **inventaire** des dispositifs mobiles qui précise, pour chaque dispositif, au moins:

- l'identification du dispositif et, le cas échéant, l'identification de la carte SIM;
- le statut du dispositif (ex.: nouveau, en réparation, attribué, à éliminer, etc.);

- l'utilisateur à qui le dispositif est attribué, ainsi que les heures de début et de fin de l'attribution, le cas échéant (ex.: des dispositifs en commun attribués à titre temporaire);
- le propriétaire (institution/BYOD).

24 Une **politique d'élimination** du dispositif est particulièrement importante pour les dispositifs mobiles. Cette politique devrait définir les obligations des utilisateurs. Elle doit également prévoir la conservation des informations, dans le cadre de l'inventaire complet des dispositifs mobiles, relatives aux dispositifs que l'on est sur le point d'éliminer. Le choix des méthodes doit reposer sur l'évaluation des brèches de sécurité associées à chaque méthode et permettre d'éliminer les dispositifs d'une manière qui garantisse en particulier que toutes les données à caractère personnel soient effacées si les dispositifs sont retirés.

IV.1.2. Politique de sécurité de l'information

25 Les institutions européennes concernées devraient adopter une politique de sécurité de l'information, et plus particulièrement une **politique de sécurité des dispositifs mobiles**, ainsi que la **déclaration de confidentialité** (claire et complète) qui s'y rattache.

> *La participation des membres de l'encadrement des institutions européennes est capitale pour le succès de la politique, laquelle devrait refléter les décisions et la culture de l'institution européenne concernée en matière de sécurité. Toutes les politiques de sécurité devraient tenir compte des exigences propres à la protection des données.*

26 Les responsables de la sécurité et les DPD doivent participer à la rédaction des politiques de sécurité et des déclarations de confidentialité dès les tout premiers instants.

IV.1.3. Formation

27 Un **plan de formation** devrait être élaboré pour sensibiliser à la manière de protéger les données à caractère personnel sur les dispositifs mobiles lorsque l'utilisation de ceux-ci est permise aux membres du personnel.

> *Cette formation est particulièrement importante pour les membres de l'encadrement, car ceux-ci sont susceptibles d'avoir accès aux données les plus sensibles dans l'organisation. Ils doivent également être conscientisés à leur responsabilité personnelle et financière éventuelle en cas de manquement aux obligations en matière de protection des données, de la même manière qu'ils sont responsables au titre du règlement financier.*

28 Ce plan de formation devrait respecter les politiques relatives aux dispositifs mobiles de l'institution européenne concernée et peut éventuellement inclure les scénarios et thèmes suivants:

- les caractéristiques de base, celles en matière de sécurité et celles en matière de vie privée des dispositifs mobiles;

- les applications et les services liés à l'entreprise;
- l'utilisation et la sécurité hors des locaux (voyage);
- l'utilisation à des fins personnelles de dispositifs appartenant à l'institution;
- le BYOD.

29 Le plan de formation devrait faire l'objet d'évaluations et de mises à jour régulières.

30 La formation peut être obligatoire à intervalles réguliers, comme un «cours de mise à niveau» pour chaque utilisateur de dispositif mobile.

IV.1.4. Mesures organisationnelles en matière de BYOD

31 Mettre en place, au niveau de l'organisation, des structures et des procédures qui garantissent l'application des politiques de l'organisation aux dispositifs (par exemple, des limitations applicables au type ou à la version du dispositif, au type de système d'exploitation, aux configurations, etc.).

32 Proposer aux utilisateurs une aide à la configuration des dispositifs de sorte qu'ils respectent les critères de sécurité, vie privée et protection des données imposés par les politiques relatives aux dispositifs mobiles.

IV.1.5. Brèches de sécurité/incidents liés à la sécurité

33 Des procédures de sécurité doivent exister pour réagir rapidement et efficacement au moindre incident lié à la sécurité (comme la perte ou le vol d'un dispositif mobile). Ces procédures doivent tenir compte des exigences propres à la protection des données et associer le DPD.

34 Les utilisateurs doivent savoir comment et à qui signaler des incidents liés à la sécurité, comme la perte ou le vol du dispositif. Une attention particulière doit être portée au fait que les utilisateurs ne seront généralement pas présents dans le bureau au moment de l'incident, raison pour laquelle des moyens adéquats doivent être prévus pour signaler des incidents liés à la sécurité; ces moyens doivent couvrir toutes les situations raisonnables dans lesquelles un utilisateur pourrait se trouver.

IV.2. Mesures techniques

35 Il existe plusieurs risques liés au traitement de données à caractère personnel. La plupart du temps, la meilleure solution, voire même la seule, à certains de ces problèmes consiste à évaluer avec minutie les applications installées sur un dispositif mobile et à configurer correctement les systèmes d'exploitation ainsi que les applications[6].

36 La gestion et la configuration des dispositifs, systèmes d'exploitation et applications échoyaient traditionnellement aux professionnels spécialisés du service informatique.

[6] Pour plus d'informations à ce sujet, voir les prochaines lignes directrices du CEPD sur la protection des données à caractère personnel traitées sur les sites web gérés par les institutions et organes de l'UE, et l'avis du groupe de travail «article 29» sur les applications destinées aux dispositifs intelligents, adopté le 27 février 2013.

Depuis l'apparition des dispositifs mobiles, souvent dans le cadre du BYOD, une partie de ces tâches échoit désormais directement aux utilisateurs qui, souvent, ne sont ni des spécialistes de l'informatique ni des experts de la sécurité/protection de la vie privée.

37 Pour résoudre cette problématique, deux méthodes devraient être appliquées conjointement par les institutions européennes concernées, à savoir:

- accroître la connaissance des risques pour la protection des données et des contre-mesures disponibles par les utilisateurs et sensibiliser davantage ces derniers[7]; et
- recourir à des solutions de «gestion des dispositifs mobiles» (GDM) adéquates, des mesures techniques qui répondent aux exigences propres à la sécurité et à la protection des données.

IV.2.1. Gestion des dispositifs mobiles (GDM)

38 Les solutions de gestion des dispositifs mobiles (GDM) peuvent servir au service informatique d'une institution européenne pour accomplir certaines tâches liées à la configuration et à la gestion de dispositifs mobiles à des fins de sécurité[8]. Néanmoins, cette possibilité fait peser des responsabilités plus nombreuses sur l'institution européenne concernée, puisque ce type de logiciel entraîne un traitement des données à caractère personnel plutôt intrusif (par exemple, la GDM peut permettre de suivre les dispositifs mobiles en temps réel). Il est par conséquent essentiel de respecter les exigences propres à la protection des données.

39 Une **solution de GDM** devrait généralement **inclure les caractéristiques suivantes**:

- sécurité:
    - utilisation obligatoire d'un code PIN/mot de passe pour accéder au dispositif mobile, applications ou conteneurs spécifiques et clés personnelles;
    - verrouillage et suppression à distance (soit de toutes les données présentes sur le dispositif, soit des seules informations relatives à l'institution);
    - détection de toute modification de la configuration;
    - accès restreint des utilisateurs et des applications au matériel du dispositif;
    - accès restreint des utilisateurs et des applications aux services du SE d'origine;
    - journaux et pistes d'audit sécurisés des activités de gestion du BYOD;

[7] Lorsqu'il existe un risque particulier ne permettant plus de garantir la sécurité, l'article 35, paragraphe 2, du règlement impose aux responsables du traitement d'informer «*les utilisateurs de l'existence de ce risque ainsi que des mesures susceptibles de l'éliminer et des autres moyens de communication susceptibles d'être utilisés*».

[8] Bien qu'autrefois, les solutions de GDM trouvaient une application dans la surveillance de l'utilisation de téléphones portables et à des fins de facturation, dans les présentes lignes directrices nous considérons que ces solutions répondent à un objectif de sécurité, et ne visent pas une utilisation à des fins de surveillance. Pour cette question, voir les lignes directrices du CEPD sur les communications électroniques (note de bas de page 4).

- sauvegarde et restauration des informations appartenant à l'institution dans le dispositif mobile;
- contrôle de conformité avant d'accéder à des ressources appartenant à l'institution;
- chiffrement des données tant en mode veille (dans le dispositif) qu'en activité (chiffrement des communications);
- distribution et gestion des certificats numériques;

- gestion du dispositif:
  - exécution centralisée de la politique de sécurité;
  - distribution sans fil de logiciels (applications et mises à jour) et modifications de la politique;
- gestion des applications:
  - verrouillage et suppression de l'application à distance;
  - listes d'applications autorisées et interdites;
  - boutiques d'applications propres à l'entreprise;
  - distribution sécurisée des applications avec contrôles adéquats des modifications non autorisées;
  - inventaire des applications par dispositif (appartenant aussi bien à l'institution qu'au particulier);
  - sécurité des applications.

40 Il est possible que les systèmes de GDM ne permettent pas de configurer ces caractéristiques sur l'ensemble des dispositifs mobiles existants, mais seulement sur certains. Il convient d'en tenir compte avant de décider quels dispositifs mobiles autoriser.

41 Lorsqu'une solution de GDM est appliquée, il y a lieu de prendre les mesures suivantes:

- évaluer l'incidence de la solution de GDM sur la protection des données;

> *Dans le cadre de cette évaluation, il importe de déterminer quelles sont les données à caractère personnel collectées par la solution de GDM et les finalités auxquelles elles sont destinées, l'emplacement et la durée de leur stockage, les personnes qui ont accès aux données et les capacités d'enregistrement. L'institution européenne concernée vérifie si ces informations sont strictement nécessaires à la finalité envisagée ou s'il existe des solutions moins intrusives.*

- informer les utilisateurs, dans la politique d'utilisation acceptable, du recours à la solution de GDM sur leur dispositif, du type d'information collectée par ce moyen et de la finalité de cette opération;

La solution de GDM que l'institution européenne concernée est libre de mettre en place pour garantir la sécurité de ses données traitées par les membres du personnel sur leurs dispositifs personnels peut entraîner un durcissement de la surveillance des membres du personnel sur leur lieu de travail par l'institution européenne concernée. Cette surveillance pourrait inclure, par exemple, l'enregistrement de la géolocalisation du dispositif mobile ou le contrôle du trafic Internet sur ledit dispositif.

- restreindre l'accès à la console d'administration de la solution de GDM selon le principe du moindre privilège et du «besoin de savoir»[9];
- évaluer la portée de la solution de GDM par rapport à l'inventaire complet des dispositifs mobiles et à d'autres sources d'information, comme les applications ou les journaux de réseau.

IV.2.2. Autres mesures techniques

42 Une solution de GDM ne répondra pas d'elle-même à tous les risques associés à l'utilisation de dispositifs mobiles. La liste suivante propose des mesures techniques pouvant être envisagées, en fonction des risques propres à chaque institution européenne. Une solution de GDM faciliterait la mise en œuvre de certaines de ces mesures, mais n'est pas nécessaire à leur fonctionnement. Ces mesures de sécurité doivent également être envisagées en tenant compte du dispositif qui est visé: le chiffrement peut s'appliquer aux dispositifs de stockage portables, comme les clés USB, au contraire d'un programme contre les logiciels malveillants, du moins en ce qui concerne la clé USB en elle-même.

43 T1: concevoir, appliquer et maintenir une solution de «sandboxing», compartimentage ou virtualisation pour séparer les informations privées et institutionnelles.

Le «sandboxing» met en place un environnement étroitement contrôlé sur un dispositif mobile dans lequel les applications peuvent fonctionner. Grâce au compartimentage, une mémoire de données chiffrées est créée sur le dispositif mobile. L'accès aux informations contenues dans le compartiment sécurisé nécessite une authentification qui s'ajoute à un éventuel autre système d'authentification déjà présent sur le dispositif mobile.

44 T2: élaborer, appliquer et tester une solution de chiffrement devant garantir que les données à caractère personnel stockées sur les dispositifs mobiles (ou, du moins, dans le «compartiment institutionnel» du dispositif, lorsqu'une solution de compartimentage/GDM existe) sont chiffrées.

45 Cette solution peut comprendre:

- l'exigence de chiffrement intégral du disque pour tous les dispositifs et de chiffrement supplémentaire pour les conteneurs d'applications sécurisés;
- l'exigence d'utilisation exclusive d'algorithmes de chiffrement classiques;

[9] *Besoin de savoir*: l'accès de l'utilisateur aux informations doit être nécessaire à l'exécution des tâches de celui-ci. *Moindre privilège*: les droits d'un utilisateur par rapport à certaines informations (lire, écrire, etc.) doivent correspondre au minimum nécessaire à l'exécution des tâches de celui-ci.

- une longueur des clés de chiffrement choisies conforme aux exigences propres à la sécurité.

46 T3: élaborer, appliquer et tester une solution de sauvegarde pour garantir la disponibilité des informations stockées uniquement sur le dispositif mobile.

> *Dans la plupart des cas, le dispositif mobile n'est pas le principal outil de stockage des informations professionnelles et la configuration du dispositif est assurée depuis un dépôt central qui rend les sauvegardes superflues. D'autre part, les données à caractère personnel (comme les données de contact) sont parfois enregistrées seulement sur le dispositif mobile, ce qui peut rendre leur sauvegarde nécessaire.*

47 T4: concevoir et imposer un procédé d'authentification de l'utilisateur approprié sur le dispositif mobile, y compris des codes PIN et des mots de passe pour déverrouiller le dispositif mobile.

> *Les utilisateurs ayant accès à des informations sensibles sont susceptibles d'être soumis à un deuxième facteur d'authentification, qui s'ajoute au code PIN/mot de passe.*
>
> *Le dispositif mobile devrait être bloqué et/ou formaté après un nombre prédéfini de tentatives infructueuses d'insérer le code PIN/mot de passe.*

48 T5: désactiver les fonctionnalités inutiles.

> *Par exemple, désactiver par défaut les fonctionnalités inutiles ou à risque comme le GPS, la communication en champ proche, le Bluetooth, etc. En désactivant les fonctionnalités inutiles, on renforce la sécurité du dispositif mobile en réduisant la surface d'attaque qui peut être exploitée pour compromettre le dispositif et on facilite l'entretien du dispositif mobile grâce au nombre réduit de composants.*

49 T6: appliquer une configuration par défaut sécurisée et respectueuse de la vie privée pour les dispositifs mobiles et les applications.

> *Par exemple, le verrouillage automatique du dispositif mobile lorsqu'il est inactif.*

50 T7: veiller à mettre à jour régulièrement les logiciels du dispositif mobile et des applications installées (à l'aide d'une solution de GDM ou non).

51 T8: autoriser l'accès aux réseaux internes des institutions européennes seulement après avoir validé la connexion réseau à partir d'un dispositif mobile en consultant le répertoire et les autorisations de l'institution.

> *Les certificats numériques du dispositif et/ou les certificats numériques de l'utilisateur peuvent servir à identifier et authentifier le dispositif mobile/utilisateur avant d'autoriser l'accès au réseau.*
>
> *Il est possible d'appliquer deux facteurs d'authentification aux connexions à des applications ou informations sensibles.*

52 T9: n'autoriser que le trafic chiffré entre les dispositifs mobiles et le réseau interne de l'institution européenne concernée.

Les utilisateurs doivent être au courant que les RPV (réseaux privés virtuels) utilisés pour le chiffrement du trafic entre le dispositif mobile et le réseau interne peuvent rediriger tout le trafic, y compris les communications privées, vers le réseau informatique de l'institution européenne concernée.

53 T10: utiliser des pare-feux courants et des applications contre les logiciels malveillants sur les dispositifs mobiles et empêcher l'accès au réseau de l'institution par des dispositifs dépourvus de tels pare-feux et applications et/ou dont la configuration est obsolète. Tant les pare-feux que les applications contre les logiciels malveillants doivent être mis à jour régulièrement (automatiquement ou non, à l'aide d'une solution de GDM ou directement auprès du vendeur du pare-feu ou de l'application).

54 T11: selon la politique d'utilisation, empêcher l'utilisation d'applications tierces pour traiter les données à caractère personnel des institutions européennes, sauf si les politiques de l'institution le prévoient et après une évaluation appropriée des risques pour les données à caractère personnel.

V. Problèmes relatifs à la protection des données dans le cadre du traitement de données à caractère personnel au moyen de dispositifs mobiles

V.1. Les institutions européennes: responsables du traitement et de la protection des données en vertu du règlement

55 Dans le cadre des activités de traitement réalisées au moyen de dispositifs mobiles, il est particulièrement important de signaler que les données à caractère personnel[10] désignent toute information concernant une personne physique identifiée ou identifiable: il s'agit non seulement des données concernant le personnel des institutions européennes, mais également des données concernant les personnes physiques hors du cadre d'une relation de travail avec les institutions ou agences européennes.

Par exemple, les dispositifs pourraient être utilisés pour offrir un accès mobile au compte de messagerie électronique professionnel de l'utilisateur, ou un accès à une base de données contenant des données à caractère personnel, et télécharger ou synchroniser ces informations vers le dispositif mobile. Les applications mobiles professionnelles pourraient être installées sur le dispositif pour accéder à des bases de données ou des portails en ligne sur lesquels différentes catégories de données à caractère personnel pourraient être également disponibles (par exemple, un système de gestion des ressources humaines).

[10] Voir définition à l'article 2, point a), du règlement. Voir également l'avis 4/2007 du groupe de travail «article 29» sur la protection des données, sur le concept de données à caractère personnel adopté le 20 juin.

Les données à caractère personnel en question pourraient ainsi désigner des noms, adresses de messagerie électronique, numéros de téléphone, informations sur le trafic et la localisation, adresses IP et témoins de connexion (cookies), pour autant qu'ils permettent d'identifier une personne physique. Il convient également de noter que les données à caractère personnel peuvent être traitées sous toutes les formes, par exemple dans un message électronique contenant des données à caractère personnel, et à l'aide de toutes les technologies, entre autres des protocoles Internet. Même dans le cas le plus simple, à savoir lorsque le dispositif n'est utilisé qu'à des fins de communications téléphoniques et d'envoi de SMS, les informations sur le trafic et les coordonnées de contact des utilisateurs du téléphone et de leurs partenaires de communication seront traitées. En outre, les smartphones et les tablettes utilisent diverses techniques qui permettent d'identifier et de suivre les personnes, c'est-à-dire connaître leur emplacement physique et savoir comment elles utilisent leurs dispositifs et les applications (les services de localisation disponibles sur les téléphones portables et les tablettes collectent des informations sur l'emplacement qui permettent à des tiers de connaître précisément les déplacements des utilisateurs). En outre, il arrive que des données à caractère personnel de tiers (à savoir, les personnes hors du cadre de la relation de travail avec les institutions européennes) soient contenues dans des messages et des appels mémorisés, par exemple, dans un système de boîte vocale.

56 Les institutions européennes doivent également collecter et traiter ultérieurement des données à caractère personnel dans le cadre de la gestion des dispositifs mobiles en eux-mêmes et, souvent, il arrive qu'elles installent également des logiciels prévus à cet effet. C'est le cas de l'installation des solutions de gestion des dispositifs mobiles (GDM), qui ajoutent des fonctionnalités pour la collecte de données et les interventions liées à la sécurité sur les dispositifs, en les connectant à des serveurs de contrôle centraux dédiés.

57 Lorsqu'un membre du personnel d'une institution européenne utilise un dispositif mobile pour des tâches professionnelles suivant les instructions de l'institution européenne concernée, celle-ci est responsable du traitement car elle fixe les finalités et les moyens du traitement de données à caractère personnel. Le traitement réalisé au moyen du dispositif mobile s'inscrit dès lors directement dans le champ d'application du règlement.[11]

58 Dans le scénario BYOD également, plus problématique que le scénario institutionnel en raison du contrôle moindre de l'institution européenne concernée sur le dispositif mobile, l'institution reste chargée de prendre toutes les mesures nécessaires pour respecter les obligations qui lui incombent en vertu du règlement et pour mettre en place le mécanisme interne servant à prouver que ces obligations sont respectées.

[11] Notons, pour donner un exemple de l'application du règlement, que si - dans ce scénario - le dispositif mobile est utilisé pour tourner des vidéos ou prendre des photos, l'institution européenne concernée doit alors tenir compte des questions soulevées dans les lignes directrices thématiques du CEPD en matière de **vidéo-surveillance** au point 2.3.1, «Les lignes directrices couvrent-elles les dispositifs autres que les systèmes de télévision en circuit fermé (CCTV)?»: «[l]'utilisation de tout autre dispositif ou système, fixe ou **mobile**, relève [...] aussi du champ d'application de ces lignes directrices si ce système est capable d'enregistrer des images» (gras ajouté).

59 Les institutions européennes doivent veiller à ne pas oublier que le traitement au moyen de dispositifs mobiles doit observer les mêmes exigences et principes que les opérations de traitement dans l'environnement de bureau «traditionnel».

60 Le membre du personnel d'une institution européenne qui utilise son propre dispositif pour exécuter des tâches professionnelles (BYOD) a l'obligation d'appliquer les politiques spécialement adoptées par l'institution européenne concernée dans ce contexte.

61 Conformément au principe de responsabilité, il importe que le DPD soit associé dès le début à la planification et à la gestion du traitement de données au moyen de dispositifs mobiles afin de garantir que les mesures prises pour atténuer ou éliminer les risques pour la protection des données soient appropriées et conformes au règlement.

62 Les **scénarios** suivants peuvent ainsi être considérés comme les principaux exemples de traitement de données à caractère personnel par l'utilisation de dispositifs mobiles:

- le traitement de données par les institutions européennes (ou leur personnel) à l'aide de dispositifs mobiles (dispositifs appartenant à l'institution européenne concernée, ou dans le scénario du BYOD), outil pour des opérations de traitement de données semblables aux opérations déjà menées par les institutions européennes dans l'environnement informatique traditionnel (bureau);
- le contrôle de l'utilisation qu'ont les membres du personnel du dispositif mobile par les institutions européennes[12];
- le traitement de données à caractère personnel dans le cadre du déploiement de solutions de GDM.

63 Dans chacun des cas précités, le règlement s'applique.

64 Le considérant 12 du règlement dispose qu'il «y a lieu d'assurer dans l'ensemble de la Communauté une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel». Ces règles désignent entre autres la directive «vie privée et communications électroniques» (directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques). Sans préjudice des dispositions particulières, ces règles sont une référence pour les institutions européennes. À cet égard, il est important de considérer ce qui suit: «en cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard indu l'autorité nationale compétente de la violation. Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard

[12] Ce scénario n'entre pas dans le champ d'application des présentes lignes directrices, mais est abordé dans les lignes directrices du CEPD sur les communications électroniques (note de bas de page 4).

indu l'abonné ou le particulier concerné de la violation.» - Article 4, paragraphe 3, de la directive 2002/58/CE (telle que modifiée par la directive 2009/136/CE). Ces règles ne s'appliquent pas directement aux institutions et organes de l'UE, mais peuvent être vues comme des bonnes pratiques (voir point V.4 ci-dessous).

65 Le règlement établit les conditions dans lesquelles le traitement de données à caractère personnel est licite. Le responsable du traitement[13] doit faire en sorte que les membres du personnel n'utilisent pas les dispositifs mobiles dans le cadre d'un traitement non couvert par une **base juridique**[14].

66 **La nécessité et la proportionnalité** du traitement de données à caractère personnel à l'aide de dispositifs mobiles contraignent les institutions européennes à mettre en balance au cas par cas les avantages de ces outils et les risques et le caractère intrusif éventuellement associés à ce traitement. Cette appréciation devrait tenir compte des fonctionnalités et caractéristiques supplémentaires du dispositif mobile, par exemple la possibilité d'étoffer la liste des contacts par des photos prises à l'aide du dispositif mobile.

67 Les utilisateurs des dispositifs mobiles doivent être **informés**[15] du traitement de données qui résulte de leur utilisation de dispositifs mobiles, que ceux-ci appartiennent à l'institution ou qu'il s'agisse de dispositifs personnels, a fortiori lorsque des données à caractère personnel sont collectées et traitées ultérieurement pour la gestion des dispositifs mobiles en eux-mêmes. Les institutions européennes devraient adopter une politique d'utilisation acceptable des dispositifs mobiles qui devrait prévoir:

- des utilisations de dispositifs mobiles clairement définies et approuvées par l'institution européenne concernée,
- les conséquences d'un usage non autorisé des ressources mobiles,
- les données à caractère personnel et informations de l'institution qu'il est autorisé de stocker et de transférer sur des dispositifs mobiles,
- le type et la version des dispositifs mobiles et systèmes d'exploitation autorisés,
- les applications qu'il est permis d'installer et d'utiliser,
- la politique de l'institution européenne concernée relative à l'utilisation de services en nuage,
- la politique de retour et d'élimination,
- une description claire des responsabilités de l'utilisateur et de l'institution européenne concernée,

[13] Comme il est expliqué à la section V.1, l'institution européenne concernée est responsable du traitement car elle fixe les finalités et les moyens du traitement de données à caractère personnel.
[14] Voir article 5 du règlement. Dans de nombreux cas, le traitement prendra comme base l'article 5, point a), qui comprend le traitement de données à caractère personnel nécessaires pour la gestion et le fonctionnement de l'institution (considérant 27).
[15] Article 11 et/ou article 12 du règlement.

- les conditions dans lesquelles le contrôle de l'utilisation de dispositifs mobiles par les membres du personnel de l'UE est autorisé, et
- une mention sur les données à caractère personnel que l'utilisateur a le droit de collecter et de traiter à l'aide de son dispositif mobile.

68 Les utilisateurs doivent accepter formellement la politique d'utilisation acceptable avant de pouvoir utiliser les dispositifs mobiles. En cas de modifications de la politique d'utilisation acceptable, il convient de communiquer sans tarder la nouvelle version aux utilisateurs qui devront l'accepter à nouveau.

69 Dans le scénario BYOD, tous les utilisateurs potentiels du BYOD doivent avoir facilement accès à la politique relative au BYOD avant de décider d'utiliser ou non leurs propres dispositifs mobiles à des fins professionnelles. Cette politique doit inclure le respect du consentement préalable à la politique, en outre de la politique d'utilisation acceptable pour tous les dispositifs mobiles, comme condition à l'autorisation du BYOD et le consentement préalable de l'utilisateur à la gestion des systèmes et au contrôle des dispositifs BYOD.

70 La configuration du dispositif mobile doit refléter («intégrer») les règles (y compris les principes de protection des données dès la phase de conception et de protection de la vie privée par défaut, et le principe de la minimisation des données). Quant à l'application du principe de spécification/limitation de la finalité, il importe d'éviter tout «détournement d'usage» (la collecte et le traitement de données à des fins secondaires non autorisées), par exemple en interdisant l'installation d'applications qui sont inutiles aux tâches professionnelles et en séparant les données professionnelles des données personnelles.

71 Quelle que soit la base juridique applicable à une opération de traitement donnée, il importe de faire référence - avant tout - à la finalité du traitement de données, et non au dispositif technique utilisé: **l'utilisation de dispositifs mobiles n'est pas, en tant que telle, une raison pour soumettre les opérations de traitement au contrôle préalable effectué par le CEPD en vertu de l'article 27 du règlement**. La nécessité de soumettre une opération de traitement au contrôle préalable du CEPD doit être évaluée au regard de la «finalité» du traitement, conformément à l'article 27, paragraphe 2, du règlement.

V.2. Obligations en matière de sécurité en vertu du règlement

72 Les responsables du traitement doivent prendre les mesures techniques et organisationnelles appropriées afin de garantir la sécurité d'utilisation des dispositifs mobiles. Ces mesures devraient assurer un niveau de sécurité approprié au regard des risques présentés, compte tenu des solutions techniques disponibles et des coûts liés à leur mise en œuvre[16].

73 Cela signifie que les responsables du traitement doivent mettre en œuvre un **processus de gestion des risques liés aux informations** conformément aux principes

[16] Article 22 du règlement.

établis en matière de bonnes pratiques. La première étape de ce processus consiste en une évaluation des risques, qui devrait inclure une analyse de l'utilisation des dispositifs mobiles. Cette évaluation des risques aidera à déterminer les principaux risques de sécurité et servira de base pour sélectionner les contrôles appropriés devant être mis en place afin de réduire les risques à un niveau acceptable pour la gestion. Le processus de gestion des risques doit comporter un réexamen périodique de l'évaluation des risques et de l'adéquation des garanties et contrôles.

74 Ce processus de gestion des risques liés aux informations doit être documenté de façon appropriée comme une politique de l'institution européenne concernée. Ce processus doit également être revu régulièrement afin de garantir qu'il conserve son efficacité et reste conforme aux objectifs opérationnels, qu'ils soient nouveaux ou modifiés. Les membres du personnel qui participent au processus (en particulier à l'analyse des risques de sécurité) ne devraient pas uniquement être ceux chargé des questions de sécurité au sein de l'institution européenne concernée. Les représentants des activités de base (RH, activités de base/opérationnelles) et le DPD doivent également être associés aux discussions pour veiller à ce que l'analyse tienne compte de l'incidence sur tous les aspects de l'organisation.

75 Les membres du personnel concernés doivent être clairement informés des principaux résultats du processus de gestion des risques liés aux informations et des risques de sécurité existants, tandis que l'encadrement et les principales parties prenantes pourraient bénéficier d'une communication détaillée des résultats de ce processus.

V.3. Analyse d'impact relative à la protection des données

76 Le CEPD recommande aux institutions européennes de prendre en considération l'utilisation de dispositifs mobiles lorsqu'elles réalisent une analyse d'impact relative à la protection des données. En particulier, cette analyse d'impact devrait être réalisée parallèlement à l'appréciation du risque pour la sécurité informatique et devrait, en tout état de cause, examiner les risques pour la sécurité qui s'y rapportent.

77 L'analyse d'impact devrait être réalisée notamment sur les outils de surveillance et de contrôle utilisés pour garantir la sécurité des dispositifs mobiles. Cette analyse devrait passer en revue les grands principes et les conditions générales de la protection des données énoncés dans le règlement, notamment le principe de licéité, la nécessité et la proportionnalité du traitement des données; la spécification et la limitation de la finalité; la qualité des données, la conservation des données; les informations sur les personnes concernées et leurs droits (accès, rectification, effacement, verrouillage) et les transferts de données.

V.4. Communication des violations de données

78 Le CEPD recommande aux institutions européennes d'adopter des procédures internes pour gérer les brèches de sécurité et les violations de données, qui prévoient en particulier la notification de la survenue de ces incidents par le responsable du traitement au DPD.

Par exemple, en cas de perte ou de vol du dispositif mobile donnant lieu à une violation de données à caractère personnel, le membre du personnel doit signaler l'incident en interne en appliquant la politique de l'institution européenne concernée en matière de gestion des brèches de sécurité et des violations de données. Le DPD doit examiner et documenter l'incident et les mesures prises pour y répondre en vue de futures évaluations et vérifications, et déterminer s'il est opportun d'informer le CEPD. La réponse du CEPD à de telles violations de données dépendra évidemment de plusieurs facteurs, dont la gravité de l'incident, le type et le volume de données touchées, le nombre de personnes concernées, la localisation des destinataires, etc.

V.5. Un scénario particulier: stockage secondaire de données à caractère personnel au moyen de dispositifs mobiles

79 Lorsque des données à caractère personnel sont traitées à l'aide d'un dispositif mobile, il se peut que l'utilisateur stocke des copies de données à caractère personnel provenant des systèmes d'information centraux sur le dispositif. Ce «stockage secondaire» risque d'entraîner des problèmes tenant à la qualité des données, à l'exercice des droits de rectification, verrouillage et effacement par la personne concernée et au respect de la période de conservation des données indiquée. Il peut arriver que ces données stockées sur le dispositif mobile ne soient pas exactes ou tenues à jour, alors que les données sont mises à jour dans le système de stockage central de l'institution européenne. Les risques pour l'institution européenne augmentent du fait de cette possible ignorance des opérations de traitement qui se déroulent sur un dispositif mobile.

Par exemple, un membre du service RH d'une institution européenne télécharge sur le dispositif mobile le document joint à un courrier électronique contenant les données à caractère personnel d'un collègue.

Dans un autre scénario possible, il arrive que l'utilisateur se serve d'une application qui copie dans le nuage les informations stockées sur le dispositif mobile à l'insu de l'utilisateur. Ce scénario présente d'autres risques liés à la confidentialité des données à caractère personnel qui sont traitées.

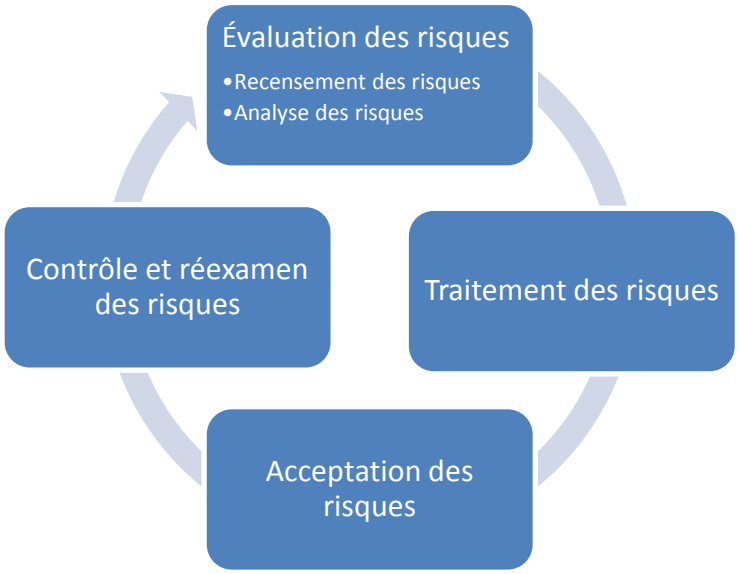
80 Si des copies locales de données à caractère personnel sur des dispositifs mobiles s'inscrivent dans l'opération de traitement telle que la conçoit l'institution européenne concernée, il est également essentiel que lorsque la personne concernée exerce le droit de rectification des données à caractère personnel inexactes ou incomplètes ou le droit de verrouillage ou d'effacement de données traitées de manière illicite, les données à caractère personnel stockées sur le dispositif mobile soient également prises en considération dans la rectification, le verrouillage ou l'effacement.

VI. Risques pour les données à caractère personnel traitées sur des dispositifs mobiles

81 Cette section propose une liste des risques et menaces qui pèsent généralement sur les données à caractère personnel présentes sur des dispositifs mobiles, et dont les institutions européennes doivent tenir compte lorsqu'elles réalisent leur propre

évaluation des risques. Cette liste offre une base sur laquelle recenser les plus grands risques et menaces, mais n'est pas exhaustive: les risques réels et les mesures de sécurité pour contrôler ces risques doivent être déterminés par chaque institution européenne dans le cadre de son évaluation.

Le diagramme suivant présente les principaux stades du processus de gestion des risques, pour rappel.



82 Les dispositifs mobiles comportent plus de risques pour les données à caractère personnel que les ordinateurs de bureau en raison de leur portabilité et, dans le cas des smartphones et tablettes, de leur capacité à collecter et à partager de grandes quantités d'informations contextuelles, de leur «connexion permanente», du nombre et de la diversité de leurs capteurs[17], et de l'attitude de l'utilisateur qui attend une «interaction continue».

83 Une utilisation mixte des dispositifs mobiles à des fins tant personnelles que professionnelles risque d'ajouter encore à la complexité. Les données à caractère personnel traitées dans le cadre de l'activité professionnelle pourraient potentiellement être traitées sans autorisation et leur confidentialité, intégrité et disponibilité pourraient être compromises par une utilisation du dispositif à des fins personnelles, et inversement, même à l'insu de l'utilisateur.

84 Les **risques** les plus inhérents aux données à caractère personnel sont les suivants:

- la perte accidentelle des données à caractère personnel;
- la modification ou la destruction des données à caractère personnel en raison d'un accès illicite aux données à caractère personnel des utilisateurs par des administrateurs des dispositifs mobiles, notamment la déconnexion à distance et la modification/suppression à distance des données à caractère personnel (photos,

[17] Par exemple: GPS, boussole numérique, gyroscope, accéléromètre, capteur de luminosité ambiante ou capteurs environnementaux, capables de mesurer la pression atmosphérique, la température et l'humidité.

vidéos, contacts locaux, copies locales de courriers électroniques, documents, etc.);

- la fuite de données à caractère personnel en raison d'un accès non autorisé à ces données, causant parfois un préjudice à l'image ou à la situation financière de l'institution européenne concernée;
- la localisation géographique illicite de l'utilisateur par des auteurs d'attaques potentielles au moyen des services de localisation;
- le vol d'identité par l'exploitation des identifiants (noms d'utilisateur, mots de passe, certificats) stockés sur les dispositifs mobiles.

85 Les **menaces** les plus courantes pouvant entraîner les risques précités sont les suivantes:

- la collecte et le traitement illicites des données à caractère personnel par les applications mobiles et/ou les dispositifs mobiles;

Ex.: localisation géographique des utilisateurs à leur insu. Analyse des échanges de sms pour établir des profils commerciaux.

- la personnalisation par les fabricants de dispositifs, transporteurs et concepteurs de SE, entraînant le verrouillage des configurations et caractéristiques;

Par exemple, l'impossibilité de désactiver les capteurs de localisation (GPS) ou de limiter les informations que le dispositif mobile transmet au vendeur du dispositif ou au fournisseur d'une application donnée.

- l'exploitation intentionnelle par des pirates informatiques (extérieurs ou infiltrés) des failles des dispositifs mobiles visant les données à caractère personnel (directement, ou conséquence collatérale d'une manœuvre visant les données professionnelles);

Ex.: un fichier PDF infecté est envoyé à l'utilisateur d'un dispositif mobile dans le but de compromettre le dispositif et d'avoir accès aux courriers électroniques de l'utilisateur.

- la perte accidentelle ou le vol du dispositif mobile;
- la modification physique non autorisée du dispositif pour accéder aux informations qu'il contient ou y installer un logiciel malveillant;

Le dispositif mobile est laissé sans surveillance dans une chambre d'hôtel ou une salle de réunion, un individu s'en empare alors et réussit à y installer des applications ou à modifier celles qui sont déjà sur le dispositif mobile ou à modifier physiquement le dispositif mobile en lui-même.

- l'usage non autorisé;

En raison d'une mauvaise configuration, l'utilisateur est en mesure de désactiver le pare-feux installé sur le dispositif mobile. Pour utiliser une application donnée, l'utilisateur désactive le pare-feux même s'il sait que la politique de l'organisation l'interdit.

- l'erreur humaine.

L'utilisateur ignore un avertissement de sécurité lancé par un dispositif mobile et le dispositif est infecté par un logiciel malveillant.

VI.1. Violation des données stockées

86 Si aucune mesure appropriée n'est en place pour sécuriser les données stockées sur les dispositifs mobiles contre les accès non autorisés ou inappropriés, l'institution européenne concernée s'expose à un risque éventuel pour son image, sa situation financière et même sa structure physique.

Quelques exemples illustrent cette menace:
• un dispositif mobile est volé, y compris les données à caractère personnel qui y sont stockées;
• un dispositif mobile ou de stockage est jeté aux ordures ou vendu sans que les données à caractère personnel soient supprimées, de sorte que la personne qui entre en sa possession peut avoir accès aux données à caractère personnel stockées dessus;
• les informations institutionnelles/personnelles stockées sur le dispositif peuvent être exposées à des applications utilisées à des fins personnelles/professionnelles;
• les applications de partage et de stockage de fichiers peuvent rendre des informations confidentielles accessibles à des tiers;
• les données à caractère personnel sont stockées sur le nuage et sont ensuite compromises.

VI.2. Traitement des «données à caractère personnel de tiers»

87 Certaines des données à caractère personnel traitées à l'aide de dispositifs mobiles se rattachent à des personnes qui n'appartiennent pas au personnel des institutions européennes: ce sont les *données à caractère personnel de tiers*.

Par exemple, un utilisateur d'une institution européenne peut avoir accès à une application institutionnelle contenant des données à caractère personnel et télécharger ces données sur le dispositif mobile. Cette nouvelle «base de données» («base de données fictive») contient les mêmes données à caractère personnel que l'application institutionnelle «d'origine», mais n'est pas protégée par les mesures de sécurité en place pour cette dernière (par ex. contrôles des accès au moyen de mesures d'authentification strictes), ou en cas de téléchargement sur l'ordinateur personnel des institutions européennes (matériel traditionnel).

88 Considérant que les dispositifs mobiles sont exposés à des risques plus grands de perte ou de vol, et que les mesures de sécurité applicables sur un dispositif mobile sont limitées, il est évident que les risques pour la protection des données sont sensiblement plus présents dans ce scénario que dans le cadre d'un accès normal à la base de données de l'institution à l'aide d'ordinateurs personnels.

VI.3. Interception de communications

89 L'interception de communications peut se définir comme l'observation ou le contrôle des communications ou activités d'une personne. Il existe généralement trois façons de surveiller les activités d'une personne: par l'écoute indiscrète des communications; par l'inspection des données collectées dans le cadre des activités de communication (métadonnées); par l'accès au dispositif mobile en lui-même.

> *Les exemples de facteurs et de procédés utilisés pour intercepter des communications incluent:*
> *• l'absence de sécurité dans les protocoles de communication pour protéger les courriers électroniques ou le trafic en ligne;*
> *• des logiciels malveillants présents sur les dispositifs;*
> *• des applications d'atteinte à la vie privée qui accèdent aux données à caractère personnel et les utilisent de manière illégitime.*
>
> *Par exemple, un point d'accès public par WiFi compromis peut servir à mener une attaque de type «man-in-the-middle» (attaque de l'intercepteur) et à extraire des informations à partir des communications entre utilisateurs.*

VI.4. Risques inhérents au BYOD

90 La possibilité donnée au personnel des institutions européennes d'utiliser («apporter») leurs propres dispositifs mobiles pour accéder aux informations de l'institution peut générer certains avantages pour les institutions européennes comme pour leur personnel. Pour autant, cette possibilité comporte également des risques supplémentaires. Le degré de contrôle que les institutions européennes et leurs services informatiques peuvent exercer - considérant également la configuration des dispositifs - peut être limité dans le scénario BYOD par rapport à un scénario dans lequel les dispositifs et les applications sont présélectionnés, approuvés et gérés par l'institution européenne concernée.

91 Si le dispositif mobile se connecte au réseau de l'institution européenne concernée, il peut entraîner un risque supplémentaire (notamment lié à l'impossibilité de gérer la sécurité du dispositif mobile). Des applications et logiciels malveillants peuvent se servir du dispositif personnel pour s'introduire dans un réseau protégé.

92 Comme il a été observé, le BYOD porte à confondre les utilisations personnelles et professionnelles. Les institutions européennes courent le risque que les données personnelles et privées des membres de leur personnel soient consultées (par ex., en accédant à des données à caractère personnel synchronisées avec l'infrastructure institutionnelle) et les membres du personnel risquent d'exposer des informations institutionnelles à travers l'utilisation de services personnels comme le stockage ou la sauvegarde sur le nuage (facile à activer par les utilisateurs eux-mêmes), ou à travers des applications installées à des fins personnelles qui peuvent, in fine, servir de «passerelles» à un accès illicite aux informations détenues par l'institution européenne concernée.

93 La variété des différents modèles de dispositifs mobiles proposés sur le marché et utilisant différents systèmes d'exploitation rend la tâche des services informatiques des institutions européennes difficile, voire impossible, services qui doivent fournir une aide dans le choix et la gestion de tous ces dispositifs. En outre, le service informatique n'aura pas le moindre contrôle sur les mises à jour et les configurations de sécurité qui peuvent être appliquées par l'utilisateur ou par le fournisseur du dispositif mobile. Quoi qu'il en soit, la complexité et la difficulté, tant sur le plan juridique que sur le plan technique, de la question de la protection des données dans le traitement de données par les institutions européennes à l'aide d'une infrastructure informatique qui se sert des dispositifs mobiles fournis aux membres du personnel ne peuvent servir de prétexte aux institutions européennes en cas de non-respect du règlement. En définitive, si le traitement de données comporte le traitement de données et d'informations particulièrement sensibles, une décision défavorable peut être envisagée par l'institution européenne concernée pour refuser, par exemple, l'utilisation de dispositifs mobiles (qu'ils appartiennent à l'institution et/ou dans le scénario BYOD) pour la collecte, le stockage et la transmission de ces données à caractère personnel.