EUROPEAN DATA PROTECTION SUPERVISOR

Lignes directrices sur la protection des données à caractère personnel pour la gouvernance informatique et la gestion informatique des institutions européennes

Mars 2018

TABLE DES MATIÈRES

SYNTHÈSE

Le règlement (CE) nº 45/2001 (ci-après le «règlement») définit le cadre juridique relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, les organes, les bureaux et les agences de l'Union européenne (ci-après les «institutions européennes»).

Les institutions européennes s'appuient sur des systèmes d'information et des bases de données pour effectuer diverses tâches opérationnelles et administratives. Une grande partie de ces systèmes d'information traitent des données à caractère personnel. Il est dès lors extrêmement important qu'ils soient pleinement conformes au règlement. En outre, en vertu du règlement général sur la protection des données (RGPD), la protection des données dès la conception deviendra pour la première fois une obligation juridique. Cela signifie que la protection des données et le respect de la vie privée devront être intégrés, dès la conception, aux spécifications et à l'architecture des systèmes et technologies d'information et de communication. Les institutions et organes de l'Union européenne seront soumis à des obligations similaires.

La finalité des présentes lignes directrices est de donner aux institutions européennes des conseils pratiques sur la manière de traiter les données à caractère personnel tout au long du cycle de vie d'un système d'information afin de garantir le respect des obligations légales des responsables du traitement des données. Néanmoins, les institutions européennes demeurent responsables du traitement adéquat des données à caractère personnel, conformément aux exigences en matière de protection des données.

Les présentes lignes directrices décrivent les aspects de la protection des données liés au traitement des données à caractère personnel par les systèmes d'information.

Elles comprennent également 26 recommandations destinées à aider les institutions européennes à renforcer les responsabilités en égard à la création, à l'exploitation et à la maintenance des systèmes d'information et des bases de données qu'elles utilisent.

La liste d'actions et de mesures recommandées dans les présentes lignes directrices ne se veut ni exhaustive ni exclusive. Les institutions européennes peuvent choisir des mesures alternatives, également efficaces, autres que celles présentées dans le présent document, compte tenu de leurs besoins spécifiques. Dans ce cas, elles devront démontrer que ces mesures offrent un niveau équivalent de protection des données à caractère personnel.

1. INTRODUCTION

1 La finalité des présentes lignes directrices est d'aider les institutions et organes de l'Union européenne (ci-après les «institutions européennes») à concevoir et à mettre en place un système de contrôle interne[1] pour la gestion et la gouvernance de leurs systèmes

[1] La démarche suivie dans les présentes lignes directrices est en adéquation avec le cadre révisé de contrôle interne de la Commission européenne [C(2017) 2373], qui structure ce contrôle en cinq composantes de contrôle interne et 17 principes. La responsabilité et la gestion des risques sont des principes de base du cadre en question ainsi que de la protection des données. Même si tous les principes s'appliquent à la gouvernance et à la gestion, les procédures informatiques sont particulièrement concernées par le principe de contrôle interne nº 11, qui traite du

informatiques[2], afin de garantir que ceux-ci et les procédures utilisées respectent les obligations juridiques qui leur incombent en matière de traitement de données à caractère personnel tout au long de leur cycle de vie, tel que défini dans le règlement (CE) nº 45/2001[3] (ci-après le «règlement»). Les présentes lignes directrices complètent celles du Contrôleur européen de la protection des données (CEPD) relatives à des questions informatiques spécifiques, portant entre autres sur les dispositifs mobiles[4], les services web[5], les applications mobiles[6] et l'informatique en nuage[7].

2 En sa qualité d'autorité de contrôle indépendante compétente pour le traitement des données à caractère personnel par les institutions européenne, le Contrôleur européen de la protection des données (CEPD) peut, entre autres tâches, publier des lignes directrices sur des questions spécifiques relatives au traitement des données à caractère personnel[8]. Les présentes lignes directrices sont le résultat d'un processus au cours duquel les institutions européenne ont été consultées.

3 En vue de garantir que les données à caractère personnel sont traitées conformément aux principes de la protection des données, la «protection des données dès la conception» et la «protection des données par défaut» constituent de bonnes pratiques de gestion des systèmes informatiques[9].

---

contrôle des technologies et de la sécurité informatique, et par le principe nº 13, qui porte sur la gestion des informations et des documents, et en particulier sur la conformité avec les règles de protection des données.

[2] Dans l'intégralité du présent document, les termes «système d'information» et «système informatique» sont interchangeables.

[3] Règlement (CE) nº 45/2001 du Parlement européen et du Conseil 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).

[4] Lignes directrices sur la protection des données à caractère personnel dans les dispositifs mobiles utilisés par les institutions européennes, 17 décembre 2015.

[5] Lignes directrices sur la protection des données à caractère personnel traitées sur les sites web fournis par les institutions européenne, 7 novembre 2016.

[6] Lignes directrices sur la protection des données à caractère personnel traitées par des applications mobiles fournies par les institutions européennes, 7 novembre 2016.

[7] Lignes directrices sur la protection des données à caractère personnel traitées par des services en nuage fournis aux institutions européennes, 16 mars 2018.

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

[9] Des orientations plus spécifiques concernant les principes de la protection des données dès la conception et de la protection des données par défaut devraient être rédigées par le comité européen de la protection des données, avec l'aide du CEPD. En outre, le CEPD prévoit de publier un avis sur les futures politiques visant à élaborer un concept plus complet de la prise en compte du respect de la vie privée dès la conception.

4 La responsabilité de la création d'un système de contrôle interne effectif incombe à la direction d'une institution. Il est recommandé que la direction prouve sa «responsabilité» en tenant pleinement compte de ses obligations.

5 À la suite de l'adoption du règlement général sur la protection des données (RGPD)[10], les principes de responsabilité, de protection des données dès la conception et de protection des données par défaut prendront de plus en plus d'importance également pour les institutions européennes, car le législateur européen a fait de ces principes des obligations légales dans le règlement susmentionné et a déclaré[11] que la législation relative à la protection des données s'appliquant aux institutions européennes sera adaptée pour tenir compte de ces mêmes principes, idéalement dans le même temps[12].

6 Les présentes lignes directrices ne peuvent pas fournir toutes les orientations nécessaires concernant l'application du principe de protection des données dès la conception à des solutions informatiques spécifiques, étant donné que des mesures techniques concrètes devront être définies et appliquées en fonction de chaque contexte technique particulier. Toutefois, intégrer également le concept de responsabilité en matière de respect de la vie privée et de protection des données dans les procédures de gestion informatique et de gouvernance informatique est une condition nécessaire pour respecter ces obligations et celles à venir.

7 Les présentes lignes directrices doivent être prises en compte par les délégués à la protection des données (DPD) et les coordinateurs ou contacts de la protection des données (CPD) au sein de chaque institution européenne, par le personnel informatique et les autres services concernés par le développement et l'exploitation des systèmes informatiques, ainsi que par toute personne agissant en qualité de responsable du traitement pour le compte des institutions européennes. Elles permettront également aux membres de la direction d'encourager une culture de la protection des données depuis le sommet de l'organisation.

8 Si les présentes lignes directrices ont pour objet d'aider les institutions européennes à remplir plus facilement leurs obligations, elles n'exonèrent pas de leurs responsabilités les institutions qui les appliquent. La liste des mesures recommandées dans les présentes lignes directrices ne se veut ni exhaustive ni exclusive. Elles sont suffisamment souples pour permettre aux institutions européennes de démarrer le processus attendu sur

---

[10] 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 (ci-après le «règlement général sur la protection des données»), JO L 119 du 4.5.2016, p. 1 à 88.

[11] Considérant 17 du RGPD.

[12] Au moment de la publication des présentes lignes directrices, la procédure législative concernant le nouvel instrument remplaçant le règlement (CE) nº 45/2001 était toujours en cours. Toutefois, il est déjà clair qu'il reflétera les dispositions pertinentes du RGPD concernant les organes de l'Union européenne. La présente version des lignes directrices fait référence au RGPD, le cas échéant. Après la publication du nouveau règlement sur la protection des données, une version actualisée faisant mention de celui-ci sera publiée.

l'obligation de rendre des comptes et d'être tournées vers l'avenir compte tenu des évolutions législatives prévues. Les institutions européennes peuvent choisir des mesures alternatives, également efficaces, autres que celles présentées dans le présent document, compte tenu de leurs besoins spécifiques. Leur efficacité devra être justifiée par écrit.

2. PORTÉE ET STRUCTURE DES LIGNES DIRECTRICES

2.1. Portée

9 Le règlement fixe les obligations des responsables du traitement des données au sein des institutions européennes en ce qui concerne le traitement des données à caractère personnel par ces mêmes institutions, et donne aux personnes des droits juridiquement protégés en matière de protection des données.

10 Le traitement des données à caractère personnel par les systèmes d'information des institutions européennes doit respecter pleinement le règlement.

11 Dans les présentes lignes directrices figurent des recommandations visant à responsabiliser davantage les institutions européennes en ce qui concerne la protection des données tout au long du cycle de vie des systèmes d'information, depuis leur création jusqu'à leur élimination, en passant par l'exploitation et la maintenance de ceux-ci. Elles contribuent à établir un système de contrôle interne pour la gouvernance informatique et la gestion informatique, qui permet au responsable du traitement des données de respecter ses obligations en matière de conformité, de vérifier celle-ci et d'en faire la preuve.

12 Les mesures proposées dans les présentes lignes directrices ne portent pas sur les aspects techniques du développement de systèmes informatiques spécifiques ou de l'utilisation d'une technologie particulière. Le CEPD continue de donner des conseils sur les questions de cet ordre dans des lignes directrices thématiques (relatives, par exemple, aux applications mobiles, aux services web, aux dispositifs mobiles et à l'informatique en nuage).

2.2. Structure des lignes directrices

13 Le chapitre 1 présente l'objet des lignes directrices.

14 Le chapitre 2 définit la portée et la structure du présent document.

15 Le chapitre 3 fournit des définitions générales de la responsabilité, de la gouvernance informatique et de la gestion informatique.

16 Le chapitre 4 présente le cadre juridique de la protection des données, ainsi qu'une vue d'ensemble des principes généralement reconnus de la protection des données qui doivent être pris en compte tout au long du cycle de vie d'un système d'information.

17 Le chapitre 5 explique comment intégrer les obligations en matière de protection des données dans le cycle de vie d'un système d'information[13].

3. PRINCIPAUX CONCEPTS: LA GOUVERNANCE INFORMATIQUE, LA GESTION INFORMATIQUE ET LA RESPONSABILITÉ

3.1. Gouvernance informatique et gestion informatique

18 Les expressions «gouvernance informatique» et «gestion informatique» désignent des fonctions centrales au sein d'une organisation. Ces fonctions ont pour objet de veiller à ce que l'environnement informatique de l'organisation soit en adéquation avec les objectifs de celle-ci.

19 *L'IT Governance Institute (ITGI) créé par l'ISACA*[14] définit la gouvernance informatique comme suit:

> *La gouvernance informatique relève de la responsabilité du conseil d'administration et des hauts dirigeants. Partie intégrante de la gouvernance d'entreprise, elle regroupe les structures et les processus organisationnels et de direction qui garantissent que les technologies informatiques de l'organisation soutiennent et amplifient les stratégies et les objectifs de cette dernière.*

20 La gouvernance informatique est orientée vers la stratégie (que faire), tandis que la gestion informatique est plus orientée vers la tactique (comment le faire). La gestion informatique englobe divers processus et fonctions.

21 Concernant l'application pratique de la gestion informatique et de la gouvernance informatique, il existe certaines bonnes pratiques telles que le référentiel ITIL[15] (Bibliothèque pour l'infrastructure des technologies de l'information) pour la gestion et le référentiel COBIT (Objectifs de contrôle de l'information et des technologies associées) pour la gouvernance.

22 Selon le référentiel COBIT [16], il convient de distinguer gouvernance et gestion:

---

[13] Le cycle de vie du modèle de système informatique utilisé comme référence dans le présent document est fondé sur le processus RUP@EC® d'IBM® (Rational Unified Process®).

[14] L'ISACA (Information Systems Audit and Control Association) est une association indépendante à but non lucratif qui défend les intérêts des professionnels travaillant dans les domaines de la sécurité de l'information, de l'assurance, de la gestion des risques et de la gouvernance. L'ISACA a créé l'ITGI dans le but d'approfondir ses recherches en matière de gouvernance informatique et autres questions connexes.

[15] Le référentiel ITIL est un cadre de bonnes pratiques destiné à la gestion du service informatique. Il reflète le cycle de vie d'un service informatique. Le référentiel ITIL est une source de conseils sur les démarches, les fonctions, les rôles et les processus, tandis qu'ISO 20000 est une norme et un code de bonne pratique. ISO 20000 - 1 fixe les exigences que se doit d'appliquer un prestataire de services pour fournir à ses clients un service de bonne qualité. ISO 20000 - 2 présente un code de bonne pratique.

[16] Le référentiel COBIT est le cadre de gouvernance et de gestion des technologies informatiques des entreprises. Il a été conçu par une équipe de travail et de développement de niveau international, issue de l'ISACA.

En ce qui concerne la gouvernance, il s'agit de veiller à ce que les besoins, les conditions et les possibilités des parties prenantes soient évalués afin de définir des objectifs d'entreprise équilibrés convenus, en fixant la direction à suivre par l'établissement de priorités et la prise de décisions, et en surveillant les performances et la conformité par rapport à la direction et aux objectifs convenus.

En ce qui concerne la gestion, il s'agit de planifier, concevoir, exécuter et surveiller les activités en adéquation avec la direction fixée par l'équipe de gouvernance pour atteindre les objectifs de l'entreprise.

23 À la suite de la centralisation des fonctions informatiques dans plusieurs institutions européennes, la création de structures de gouvernance appropriées a pris plus d'importance, car il convient de veiller à ce que les besoins et préoccupations des services de l'organisation qui n'ont plus recours à des infrastructures décentralisées distinctes soient correctement pris en compte dans la gouvernance de l'infrastructure informatique générale. En matière d'informatique, la responsabilité est une question qui concerne la structure et le processus de gouvernance.

24 Les structures et processus de gouvernance informatique doivent être conçus pour garantir la conformité avec les principes de protection des données et l'application efficace de ceux-ci. Ils devraient également porter sur les aspects organisationnels et les questions liées au personnel, par exemple définir clairement les rôles et les responsabilités et sensibiliser tous les membres du personnel aux politiques et législations en vigueur en matière de protection des données.

25 Les rôles en matière de protection des données aux différents échelons d'une institution européenne (direction ou unité, par exemple), ainsi que l'attribution des responsabilités, devraient être clairement définis dans les structures de gouvernance et de gestion informatiques de cette institution.

3.2. Responsabilité en matière de protection des données

26 Le terme «responsabilité» est utilisé dans divers contextes et sa signification a été récemment élargie pour décrire une démarche globale qui consiste à satisfaire aux exigences de protection des données au-delà de la simple conformité avec la législation.

27 Le groupe de travail de l'article 29 indique dans son avis[17] qu'en matière de responsabilité, *l'essentiel est de montrer comment celle-ci est exercée et de pouvoir le vérifier*.

28 Dans son avis[18] sur le paquet de mesures pour une réforme de la protection des données, le CEPD déclare que le principe de responsabilité met davantage l'accent sur la responsabilité du responsable du traitement. En règle générale, le responsable du

[17] Avis 3/2010 du groupe de travail «Article 29» sur le principe de la responsabilité.

[18] Avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données.

traitement doit adopter des politiques et mettre en place des mesures appropriées visant à garantir et à pouvoir *démontrer* la conformité avec les règles de protection des données et à garantir que l'efficacité de ces mesures est vérifiée.

29 Cette vérification peut être effectuée en recourant à des ressources internes telles que les services en charge de la conformité dans une entreprise et/ou les services d'audit interne, ainsi qu'à des ressources externes telles que les organismes de certification ou de codes de conduite, les cabinets d'audit etc.

30 L'article 5 du RGPD[19] traite de la responsabilité et dispose en la matière que *le responsable du traitement est responsable du respect des principes de «licéité, loyauté et transparence», de «limitation des finalités», de «minimisation des données», d'«exactitude», de «limitation de la conservation» et de sécurité («intégrité et confidentialité») en matière de protection des données, et qu'il est en mesure de démontrer que ceux-ci sont respectés*.

31 La responsabilité incombe au plus haut niveau de la direction d'une organisation, qui doit s'assurer que l'ensemble de celle-ci satisfait à ses obligations.

R1: Il est extrêmement important que les principes de protection des données soient explicitement soutenus par la direction d'une organisation.

32 Celle-ci peut déléguer la responsabilité de l'application de ses politiques en définissant clairement les mandats et les pouvoirs octroyés.

R2: Les membres de la direction, qu'ils remplissent ou non la fonction de responsable du traitement pour des opérations spécifiques de protection des données, doivent rendre des comptes en matière de protection des données. S'ils ne remplissent pas eux-mêmes la fonction de responsable du traitement, les membres de la direction sont malgré tout responsables de veiller au respect des règles de protection des données, par exemple en établissant les structures et les processus organisationnels adéquats, de manière à ce que l'équipe de gestion opérationnelle ait les moyens et l'autorité pour remplir la fonction de responsable du traitement et garantir la conformité.

33 Même si le règlement prévoit que le responsable du traitement est le seul responsable en matière de protection des données, en raison de l'introduction de la responsabilité, les membres de la direction doivent procurer au responsable du traitement de leur institution tout ce dont il a besoin pour contrôler la conformité des opérations de traitement et rectifier les problèmes.

[19] Comme expliqué au paragraphe 5, le législateur a déclaré que la législation en matière de protection des données destinée aux institutions européennes sera adaptée pour appliquer les mêmes principes, idéalement au même moment.

R3: Les membres de la direction devraient désigner un responsable[20] de la protection des données (un délégué à la protection des données ou un coordinateur de la protection des données, par exemple) et lui fournir un mandat pour mettre en œuvre les politiques de protection des données.

34 Le DPD ou le CPD ne devrait pas seulement donner des conseils aux responsables du traitement dans leur domaine de responsabilité, mais également avoir le droit d'obtenir les informations sur les opérations de traitement dont il a besoin pour effectuer son travail. De plus, il devrait être en mesure de faire part directement aux membres de la direction de ses observations concernant des opérations de traitement qui pourraient avoir une incidence sur les droits des personnes en ce qui concerne le traitement de leurs données à caractère personnel.

35 Les orientations fournies par le responsable de la protection des données concernant l'application correcte des politiques de l'organisation doivent être suivies par tous les membres du personnel associés aux processus concernés.

R4: L'ensemble du personnel devrait connaître les politiques et procédures en vigueur en matière de protection des données. Une formation d'intégration obligatoire, la distribution de documents d'information ou des formations périodiques sont des moyens d'y parvenir.

36 L'équipe de direction ne peut pas compter sur la bonne application de ses politiques si l'efficacité de celles-ci n'est pas régulièrement vérifiée.

R5: Les politiques, les procédures ainsi que les responsabilités et les fonctions concernant la protection des données devraient être régulièrement surveillées et actualisées.

37 Le responsable de la gouvernance informatique devrait être conscient de l'éventuelle existence d'une informatique de l'ombre («shadow IT»)[21]. Il convient de sensibiliser le personnel à ce problème afin d'en atténuer les effets et de garantir que les mesures de conformité portent sur tous les systèmes essentiels. Les membres de la direction devraient être avertis des problèmes liés à l'informatique de l'ombre et des risques qui en découlent.

[20] Le rôle du délégué à la protection des données est expliqué plus en détail dans les lignes directrices concernant les délégués à la protection des données (DPD) publiées par le groupe de travail «Article 29».

[21] Le terme «informatique de l'ombre» désigne les systèmes informatiques qui ne sont pas sous la responsabilité du principal service informatique de l'organisation, mais qui sont gérés et régis par un autre service opérationnel ou administratif à ses propres fins. Cette séparation complexifie souvent la vérification de la conformité avec les règles de l'organisation. L'informatique de l'ombre désigne également les systèmes informatiques utilisés par des employés avec ou sans autorisation officielle de l'organisation. Cela comprend notamment les dispositifs mobiles utilisés selon le principe «Apportez votre équipement personnel de communication», pour lesquels le CEPD formule des recommandations dans ses lignes directrices sur les dispositifs mobiles.

3.3. Protection des données dès la conception et protection des données par défaut

38 En vertu de l'article 25 du RGPD, le responsable du traitement «*met en œuvre des mesures techniques et organisationnelles appropriées [...], qui sont destinées à mettre en œuvre les principes relatifs à la protection des données [...] et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée*». Le responsable du traitement respecte cette obligation «tant au moment de la détermination des moyens du traitement» (c'est-à-dire lorsque les systèmes de traitement sont conçus, développés et testés) *«qu'au moment du traitement lui-même»* (lorsque le système de traitement est exécuté).

39 Il doit en outre garantir que, «*par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées*» (protection des données par défaut).

40 Le responsable du traitement ne peut respecter ces obligations que si la gouvernance et la gestion informatiques ainsi que les processus de développement des systèmes sont organisés de manière à ce que les considérations relatives à la protection des données soient prises en compte à chaque étape.

41 Dans la section 5, il est expliqué comment ces obligations doivent être prises en considération à chaque phase du cycle de vie d'un système informatique et dans les processus horizontaux correspondants. Cela commence par l'introduction d'exigences élevées en matière de protection des données dans la charte du projet lors de la phase de démarrage et se poursuit par la définition d'exigences fonctionnelles et non fonctionnelles de protection des données dans le cadre de la configuration du système, l'intégration des garanties et des mesures appropriées dans la conception, leur vérification au cours de tests, l'ajout de mesures appropriées, telles que des notifications et des mesures de surveillance dans les procédures opérationnelles, et la formation appropriée des utilisateurs et des autres membres du personnel concernés lorsque le système devient productif. Lors de la procédure d'acquisition de systèmes et de services informatiques, les institutions européennes, comme toute autre entité publique, sont tenues d'inclure des critères de protection des données dans les spécifications de leurs appels d'offres[22], afin d'inciter les fabricants et les fournisseurs de produits et de services à tenir compte de la protection des données dès la conception dans leur

[22] Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les sous-traitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données. Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics.

processus de développement. Une telle incitation contribuera à faire progresser l'état de la technique en matière de protection des données dès la conception.

42 En ce qui concerne les institutions européennes, la protection des données par défaut est particulièrement importante pour les systèmes qui interagissent directement avec les utilisateurs, au sein ou à l'extérieur de ces institutions. Le cas échéant, toute opération de traitement doit se limiter au strict nécessaire, ce qui s'applique «*à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité*[23]» qu'il soit question de personnes physiques ou d'organisations. Ce principe devrait également être appliqué aux fonctionnalités de suivi, dans le cas de services internet ou d'applications mobiles, par exemple.

4. CADRE JURIDIQUE DE LA PROTECTION DES DONNÉES

43 Cette section présente une vue d'ensemble des concepts fondamentaux de la protection des données qui devraient être pris en considération dans tous les processus de gestion et de gouvernance informatiques.

44 Outre le règlement, les présentes lignes directrices font également référence aux concepts du RGPD qui deviendront obligatoires pour les institutions européennes lorsque le règlement sera adapté au RGPD. Ces concepts complètent et renforcent les principes énoncés dans le règlement et sont pleinement conformes au cadre actuel. Ils sont déjà considérés comme étant de bonnes pratiques et peuvent être appliqués dans le cadre juridique en vigueur.

Données à caractère personnel

45 En vertu de l'article 2 du règlement, on entend par «données à caractère personnel»: toute information concernant une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale[24].

Personne concernée

46 Par personne concernée, on entend la personne dont les données à caractère personnel sont collectées, conservées ou traitées.

---

[23] Article 25, paragraphe 2, du RGPD.

[24] Pour obtenir de plus amples informations ainsi que des exemples, consulter l'entrée «données à caractère personnel» du glossaire du CEPD et l'avis 04/2007 du groupe de travail «Article 29» sur le concept de données à caractère personnel.

Responsable du traitement

47 Le responsable du traitement des données est l'institution ou l'organe qui détermine les finalités et les moyens du traitement de données à caractère personnel. Il est notamment chargé de veiller à la qualité des données et de notifier l'opération de traitement au délégué à la protection des données (DPD). Le responsable du traitement des données est également responsable des mesures de sécurité destinées à protéger les données.

Sous-traitant

48 On entend par «sous-traitant» la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Fondement juridique du traitement des données à caractère personnel

49 L'article 5 du règlement pose les fondements juridiques du traitement des données à caractère personnel, à savoir:

1. le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt public sur la base des traités,
2. le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis,
3. le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci,
4. la personne concernée a indubitablement donné son consentement,
5. le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée.

4.1. Exigences en matière de protection des données

50 La liste ci-dessous donne un aperçu rapide des principes généralement reconnus en matière de protection des données.

51 Ces principes forment la clé de voûte de la protection des données depuis ses origines et sont intégrés au règlement. Ils sont présentés ci-après conformément au modèle énoncé à l'article 5 du RGPD.

1. **Licéité, loyauté et transparence**[25]

- Rester transparent vis-à-vis des personnes concernées concernant le traitement de leurs données;
- Informer les personnes concernées du traitement de leurs données, par exemple, de sa finalité et de l'identité du responsable du traitement;
- Communiquer clairement aux personnes concernées la manière dont leurs données à caractère personnel seront traitées, dans quelle mesure et à quelles fins;

[25] Voir également la section 5.6.1 sur l'information des personnes concernées et la transparence.

- Vérifier qu'il existe une fondement juridique clair pour le traitement des données à caractère personnel et que le traitement respecte les limites imposées par cette base;
- Si le consentement constitue le fondement juridique, il doit être lié à une finalité, enregistré et assorti d'une possibilité de le retirer[26];
- Respecter les droits des personnes à accéder à leurs données et à les rectifier;
- Élaborer des procédures et des instructions qui expliquent clairement comment les personnes concernées peuvent exercer leur droit d'accès et de rectification à chaque phase du traitement des données;
- Intégrer des fonctionnalités dans le système informatique qui permettent de gérer les demandes d'accès, de modification ou de blocage, ainsi que les objections au traitement;
- Adopter des règles internes visant à examiner la validité du fondement juridique en cas de changement, par exemple si le consentement est retiré[27].

2. Limitation des finalités

- Traiter les données à caractère personnel uniquement pour des finalités déterminées, explicites, légitimes et limitées;
- Limiter le traitement des données par un système informatique à la finalité initiale;
- Garantir la limitation des finalités si différents types de données sont collectés et traités pour des finalités différentes;
- Adopter des règles internes relatives à l'évaluation des besoins de compatibilité au cas par cas[28] pour permettre un changement de finalité;
- Communiquer clairement aux personnes concernées tout changement de la finalité initiale du traitement de leurs données à caractère personnel.

3. Minimisation des données

- Veiller à ce que les données à caractère personnel soient adéquates, pertinentes et limitées à ce qui est nécessaire au regard de la finalité;
- Limiter les catégories de données à caractère personnel à traiter à une collecte de données ayant un rapport direct avec les finalités initiales;
- Envisager d'utiliser et utiliser si possible des technologies renforçant la protection de la vie privée, qui permettent d'éviter un usage excessif de données à caractère personnel ou d'utiliser des données anonymes.

[26] Consulter également l'entrée «consentement» du glossaire du CEPD.

[27] Consulter également l'entrée «consentement» du glossaire du CEPD.

[28] Avis 03/2013 du groupe de travail «Article 29» sur la limitation des finalités.

4. Exactitude

- Veiller à ce que les données à caractère personnel soient exactes et à jour;
- Mettre en place des procédures permettant de garantir et de préserver l'exactitude des données traitées, par exemple en vérifiant automatiquement la qualité des informations saisies dans le système avant le traitement;
- Veiller à ce que la personne concernée ait la possibilité de rectifier les données qui ne sont plus exactes.

5. Limitation de la conservation

- Conserver les données à caractère personnel pendant une durée n'excédant pas celle nécessaire au regard de la finalité initiale;
- Déterminer à l'avance la durée de conservation des données conservées sous une forme permettant l'identification des personnes concernées;
- Veiller à ce que les périodes de conservation nécessaires soient proportionnelles aux finalités de la collecte des données et limitées dans le temps, Déterminer et gérer séparément les durées de conservation des données collectées à des fins différentes;
- Faire particulièrement attention aux données à caractère personnel conservées sur papier étant donné que leur existence est difficile à repérer;
- Concevoir des fonctionnalités informatiques qui permettent de gérer les durées de conservation et d'exécuter les actions nécessaires par la suite, à savoir la suppression des données ou leur anonymisation.

6. Intégrité et confidentialité

- Veiller à la sécurité des données à caractère personnel;
- Effectuer une évaluation des risques pesant sur la sécurité et prévoir des mesures de réduction des risques[29];
- Garder à l'esprit qu'une copie papier peut contourner les mesures de réduction des risques définies pour le système informatique, par exemple des listes de contrôle d'accès;
- En fonction de l'évaluation des risques, concevoir et appliquer des mesures organisationnelles et techniques de réduction des risques à un niveau acceptable, éviter les opérations de traitement pour lesquelles ces mesures ne seraient pas efficaces, et veiller à ce que l'équipe de direction responsable décide clairement des risques qui sont acceptés et pourquoi. Étant donné que les risques relatifs à la protection des données sont liés aux droits fondamentaux d'autres personnes,

[29] Consulter par exemple les lignes directrices du CEPD sur les mesures de sécurité pour le traitement des données à caractère personnel.

l'externalisation des risques (assurance) est une option moins viable que dans d'autres domaines de risques.

7. Responsabilité

- Veiller à ce que le respect des principes énoncés ci-dessus puisse être démontré.

52 Outre ces principes, les responsables du traitement sont tenus de respecter les droits des personnes concernées en matière d'accès, de rectification, d'effacement, de restriction de traitement ou d'opposition au traitement, eu égard notamment à la prise de décision automatisée.

53 Le responsable du traitement doit respecter l'obligation de ne transférer des données à caractère personnel à des entités situées dans des pays tiers que si un niveau adéquat[30] de protection est garanti[31].

5. EXIGENCES DE PROTECTION DES DONNÉES AU COURS DU CYCLE DE VIE D'UN SYSTÈME INFORMATIQUE

54 Ce chapitre décrit le traitement des données à caractère personnel tout au long du cycle de vie d'un système informatique[32], depuis sa création jusqu'à son fonctionnement et sa maintenance, ainsi que dans les processus horizontaux tels que la gestion de projets.

55 Le tableau

[30] Voir le document d'orientation du CEPD sur le transfert de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions et organes de l'Union européenne.

[31] Voir également l'annexe 1 sur le traitement par des organisations externes et les transferts de données à caractère personnel.

[32] Le cycle de vie du système informatique utilisé comme référence dans le présent document est fondé sur le processus RUP@EC® d'IBM® (Rational Unified Process®); méthodologie de développement adaptée à la Commission européenne.

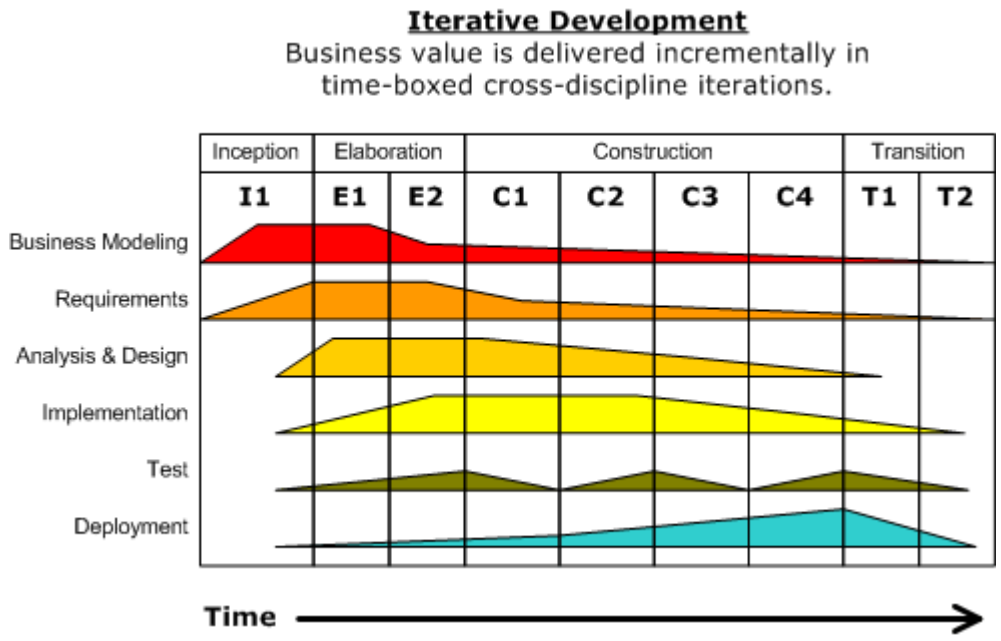

Figure 1: phases du cycle de vie (source: Dutchguilder, domaine public)

Iterative Development	Développement itératif
Business value is delivered incrementally in time/boxed cross/discipline iterations.	La valeur commerciale est fournie progressivement par itération interdiscipline délimitée par le temps.
Inception	Démarrage
Elaboration	Élaboration
Construction	Construction
Transition	Transition
I1	I1
E1, E2	E1, E2
C1, C2, C3, C4	C1, C2, C3, C4
T1, T2	T1, T2
Business modeling	Modélisation
Requirements	Exigences
Analysis & Design	Analyse et conception
Implementation	Exécution

Test	Test
Deployment	Déploiement
Time	Temps

joint à l'annexe 2 présente des recommandations importantes sur les exigences de protection des données (voir les sections suivantes) dans les différentes phases du cycle de vie d'un système informatique.

5.1. Démarrage (Commencer)

56 La phase de démarrage consiste à définir la portée du projet et à convenir de ses exigences de haut niveau.

57 Le responsable de la protection des données (le délégué à la protection des données ou le coordinateur de la protection des données, par exemple) devrait être considéré comme partie prenante dans un projet informatique et pourrait contribuer, entre autres, à faciliter la protection de toutes données à caractère personnel traitées par le système informatique concerné comme un produit final du projet. Le DPD ou le CPD devrait participer au projet dès la phase de démarrage.

R6: En premier lieu, il convient de déterminer si les données traitées par le système informatique concerné sont des données à caractère personnel ou non, ou si elles pourraient le devenir à la suite d'un tel traitement.

58 Si le traitement de données à caractère personnel est prévu, le fondement juridique de ce traitement devrait être déterminé.

59 Les risques relatifs à la protection des données et les garanties applicables devraient être déterminés à haut niveau.

R7: Les exigences élevées en matière de protection des données devraient être incluses dans une charte de projet, étant donné que ce document comporte le cahier des charges et les spécifications de haut niveau, et qu'il résulte de la phase de démarrage.

60 À ce stade, les risques élevés[33] qui pourraient peser sur le traitement de données à caractère personnel devraient être pris en considération. À la lumière de la prochaine

[33] Dans les lignes directrices du CEPD sur les mesures de sécurité pour le traitement des données à caractère personnel, un risque est défini comme étant l'effet de l'incertitude sur les objectifs. Les risques élevés sont identifiés lors de la phase de démarrage. L'analyse complète des risques est effectuée lors de la phase de planification et se poursuit tout au long du cycle de vie du projet.

révision des obligations juridiques, il est recommandé d'effectuer une analyse d'impact relative à la protection des données, conformément au RGPD.

61 Une procédure de gestion des risques devrait être menée tout au long du cycle de vie du projet[34].

5.2. Élaboration (Planifier)

62 La phase d'élaboration permet de déterminer le travail à effectuer lors des phases suivantes du projet. Au cours de ces phases, un futur système informatique sera conçu en fonction d'exigences à collecter.

5.2.1. Collecte des exigences

R8: Les exigences de protection des données devraient être recueillies auprès des parties prenantes et documentées au cours de la phase de spécification du système informatique.

63 Ces exigences devraient être conservées et révisées selon la méthodologie usuelle du cycle de vie d'un projet. Le chef de projet devrait consulter le responsable de la protection des données (le délégué à la protection des données ou le coordinateur de la protection des données, par exemple), de sorte que ce dernier puisse lui donner une vue d'ensemble complète des exigences de protection des données.

64 La protection des données se traduit par des exigences fonctionnelles et non fonctionnelles[35]. Dans les exigences fonctionnelles figurent en particulier les capacités nécessaires pour garantir les droits des personnes concernées, tels que le droit d'accès (article 15 du RGPD), le droit à la portabilité des données (article 18 du RGPD), le droit de rectification (article 16 du RGPD) et le droit à l'effacement (article 17 du RGPD), ainsi que des fonctionnalités permettant de garantir la limitation de la durée de conservation des données [article 5, point e), du RGPD]. Les exigences non fonctionnelles portent sur le respect des principes de minimisation des données et de limitation des finalités [article 5, points b) et c), du RGPD], qui doivent être pris en considération lors de la conception des structures de données d'un système, ainsi que sur des objectifs généraux tels que la sécurité et la vérifiabilité.

65 L'intégration des exigences de protection des données dans cette phase est une condition préalable à la prise de décisions appropriées lors de la phase de conception.

[34] Voir note de bas de page nº 33.

[35] Les exigences non fonctionnelles sont également considérées comme des exigences de qualité en vertu de la norme ISO 25010.

5.2.2. Conception

66 La phase de conception permet de déterminer comment les exigences seront réellement mises en place dans le système. Lors de cette phase, les éléments de base et les fonctionnalités du système sont définis, ainsi que leurs interactions. C'est également au cours de cette phase que les mesures de sécurité nécessaires pour protéger les données à caractère personnel traitées seront définies, par exemple.

67 Il est important que le personnel technique participant à un projet informatique, ainsi que les spécialistes de la protection des données soient au fait des dernières évolutions des technologies et des produits permettant de répondre aux exigences de protection des données.

68 Grâce au nouveau cadre de protection des données, la «protection des données dès la conception» et les technologies renforçant la protection de la vie privée deviendront des instruments obligatoires pour améliorer la protection des données[36]. Même si toutes les exigences fonctionnelles et non fonctionnelles de protection des données doivent être prises en considération dans la phase de conception, les décisions en matière de conception doivent également tenir compte des caractéristiques de protection des données des stratégies technologiques choisies. Les modules et les fonctions de réutilisation choisis ne devraient pas exécuter d'opérations de traitement, y compris la collecte de données qui ne sont pas nécessaires à la finalité du système; par exemple, les concepteurs ne devraient pas réactiver les banques de données qui ont été conçues dans l'objectif de collecter le plus grand nombre de données possible ou d'enregistrer de façon détaillée les actions des utilisateurs, de telles informations pouvant être utilisées à des fins de profilage dans d'autres circonstances. Les concepteurs devraient également éviter d'utiliser des outils qui communiquent des données à caractère personnel à des tiers. Lorsqu'il est possible de recourir à des technologies qui contribuent à renforcer la protection des données, celles-ci devraient être privilégiées par rapport aux autres technologies favorisant moins le respect de la vie privée. Cette stratégie permettra de créer des systèmes informatiques suffisamment souples pour garantir une protection adéquate des données à caractère personnel.

69 Lorsque le volume de traitement peut être déterminé par la personne concernée, les valeurs d'initialisation des paramètres en question seront définies de manière à exécuter les opérations de traitement les plus limitées possible, et l'utilisateur doit avoir la possibilité de choisir un traitement plus complet, s'il le souhaite.

70 L'article 22, paragraphe 2, du règlement répertorie un ensemble d'objectifs de sécurité et de risques génériques qui doivent être réduits. Le responsable du traitement

[36] En vertu du règlement général sur la protection des données (RGPD), la protection des données dès la conception devient pour la première fois une obligation légale pour les responsables du traitement des données et les sous-traitants.

appliquera des mesures permettant d'atteindre ces objectifs et de réduire ces risques, ainsi que toute perte de confidentialité, d'intégrité et de disponibilité susceptible de compromettre des données à caractère personnel. Le choix de contremesures dépendra du résultat de l'évaluation des risques spécifiques[37].

71 Par exemple, les contrôles d'accès garantissent que seules les personnes autorisées sont en mesure de lire, de modifier ou de supprimer des données dans le système. De tels contrôles contribuent à assurer la confidentialité et l'intégrité des données du point de vue de la sécurité. De plus, lorsqu'un système informatique traite des données à caractère personnel, les contrôles intégrés devraient garantir que les utilisateurs n'ont accès qu'aux données nécessaires à l'exécution de leurs tâches. Les contrôles d'accès peuvent ainsi contribuer à garantir que l'utilisation des données à caractère personnel est limitée aux fins autorisées (limitation des finalités) et que les données sont protégées de tout accès non autorisé et de toute altération.

R9: Des mesures de sécurité supplémentaires, telles que le cryptage et les contrôles d'accès multiniveaux, devraient être mises en place pour réduire les risques élevés liés au traitement informatique de données (à caractère personnel) particulièrement sensibles, relatives, par exemple, à la santé physique ou mentale, à l'origine raciale ou ethnique, aux opinions politiques, aux croyances religieuses ou aux décisions pénales.

72 Plusieurs mesures peuvent être en place pour garantir la sécurité. Des mots de passe peuvent être demandés pour accéder à des fichiers personnels. Concernant l'identification des utilisateurs autorisés, des procédures d'ouverture de session distinctes ainsi que des journaux consignant les accès aux fichiers et les modifications des données devraient être mis en place.

R10: Des fonctionnalités adéquates devraient être intégrées au système informatique afin de pouvoir gérer correctement les durées de conservation et exécuter les actions nécessaires par la suite, par exemple l'anonymisation ou la suppression de données.

73 Dans son avis 5/2014 sur les techniques d'anonymisation[38], le groupe de travail «Article 29» conclut «*que les techniques d'anonymisation peuvent apporter des garanties en matière de respect de la vie privée et peuvent servir à créer des procédés d'anonymisation efficaces, mais uniquement si leur application est correctement conçue – ce qui suppose que les conditions préalables (le contexte) et le(s) objectif(s) du processus d'anonymisation soient clairement définis de façon à parvenir à l'anonymisation visée, tout en produisant des données utiles. Le choix de la solution optimale devrait s'opérer au cas par cas, en utilisant éventuellement une combinaison*

[37] Consulter par exemple les lignes directrices du CEPD sur les mesures de sécurité pour le traitement des données à caractère personnel.

[38] Avis 05/2014 du groupe de travail «Article 29» sur les techniques d'anonymisation.

de techniques différentes, sans perdre de vue les recommandations pratiques formulées dans cet avis».

5.3. Construction et développement (Réaliser)

74 Durant la phase de développement, le code est écrit et, si le système comporte du matériel, sa conception et sa configuration seront alors aussi réputées satisfaire aux obligations découlant de l'évaluation des risques.

> R11: Il est important d'établir une entente commune entre l'équipe de développement et les parties prenantes. Cette équipe devrait être au fait de la législation et des règles relatives à la protection des données avant que ne commence la phase de développement. Pour s'en assurer, il peut s'avérer utile d'organiser avec le DPD une formation des membres actuels et nouveaux de l'équipe de développement, ou de mettre en place des initiatives équivalentes.

75 L'équipe de développement devrait documenter la création du système de manière complète et compréhensible.

5.4. Test (Contrôler)

76 La phase de test permet de vérifier si le système en cours de développement satisfait à toutes les exigences.

77 Les exigences de protection des données devraient être examinées dans le cadre de cas et de scénarios d'essai.

78 Les tests devraient également cibler toutes les exigences de protection des données concernées, par exemple l'existence d'un avis de protection des données clair et exhaustif, de fonctionnalités permettant de gérer la qualité des données et les cookies, de paramètres par défaut favorables au respect de la vie privée, ainsi que les exigences en matière de sécurité informatique.

79 Une approche intégrée des essais de sécurité dans la phase de développement (avec une analyse du code statique de sécurité et des approches dynamiques telles que des essais de pénétration) peut jouer un rôle essentiel.

> R12: Les procédures et les instructions de test devraient être élaborées de manière à garantir l'adéquation avec les exigences de protection des données.

80 Lors de la phase de test, il convient d'éviter l'échantillonnage de données à caractère personnel réelles, car celles-ci ne peuvent pas être utilisées à des fins pour lesquelles elles n'ont pas été collectées et les utiliser dans le cadre de tests pourrait les rendre accessibles à des personnes non autorisées.

81 Il est recommandé d'utiliser, si possible, des données artificiellement créées ou des données de test qui sont dérivées de données réelles, dont la structure a été préservée

mais qui ne contient en fait aucune donnée à caractère personnel. Différentes techniques de ce genre ont été appliquées avec succès[39].

82 Lorsqu'une analyse complète et prudente montre que les données de test produites ne peuvent pas suffisamment garantir la validité des tests, une décision globale doit être prise et documentée, portant sur les données réelles, limitées au maximum, qui seront utilisées dans le test, ainsi que sur les garanties techniques et organisationnelles supplémentaires qui seront mises en place dans l'environnement de test. Certaines catégories de données spéciales ne peuvent être utilisées dans des tests de données réelles qu'avec le consentement explicite des personnes concernées.

R13: Il est préférable d'éviter l'échantillonnage de vraies données à caractère personnel lors d'une simulation d'environnement réel.

83 Des mesures de sécurité efficaces devraient être prises en compte lors du test d'un système informatique. S'il est nécessaire d'utiliser de vraies données à caractère personnel pour le test, celles-ci devraient être anonymisées. La création, par les développeurs, d'ensembles de données artificielles à usage général est une alternative à considérer.

84 En cas d'utilisation de données à caractère personnel dans l'environnement de développement ou de test, les exigences en vigueur dans l'environnement de production doivent être appliquées.

85 Lorsqu'un sous-traitant tiers sous contrat participe à un test, il convient de prêter une attention particulière aux données qui sont mises à disposition pour le test. D'une manière générale, aucune donnée à caractère personnel réelle ne devrait être utilisée à cette fin.

86 Les contractants ne devraient avoir accès qu'aux environnements de test. Si l'accès à l'environnement de production est nécessaire, seuls les administrateurs informatiques autorisés[40] de l'institution concernée devraient exécuter les actions nécessaires en suivant les instructions des contractants, après que les contrôles de procédure appropriés ont été menés. Lorsque les administrateurs informatiques sont uniquement externes, le responsable du traitement doit s'assurer que le contractant respecte les exigences de protection des données applicables.

5.5. Transition et déploiement (Agir)

87 Le principal objectif de cette phase est de faire passer le système du stade du développement à celui de la production. Les utilisateurs doivent comprendre le système.

[39] Des techniques et des outils de production de données de test sont mis à disposition avec différents contextes de développement.

[40] L'octroi de privilèges d'administrateur informatique devrait être soumis à la décision d'un propriétaire du système.

Par conséquent, les activités de cette phase devraient inclure une initiative de sensibilisation à la protection des données pour les utilisateurs finaux et le personnel de maintenance.

R14: Les utilisateurs finaux, les administrateurs du système et le personnel de maintenance du système informatique devraient connaître les règles de protection des données.

5.6. Exploitation et maintenance

88 Une fois qu'un système informatique a passé avec succès la phase de test et qu'il est autorisé à la production, il intègre le fonctionnement standard de l'organisation. L'équipe de développement passera la main à l'équipe d'exploitation. Les ressources en développement ne serviront qu'à des fins de maintenance, c'est-à-dire à corriger des erreurs découvertes lors du fonctionnement productif du système et à mettre en œuvre des adaptations limitées du système en cas de modification des spécifications.

89 Contrairement au développement de systèmes, généralement organisé sous forme de projets et composé de nombreuses activités uniques, l'exploitation d'un système est un processus de fonctionnement quotidien et continu, durant lequel certaines étapes se répètent à intervalles réguliers (sauvegarde, préparation, mise à niveau, etc.).

90 L'équipe d'exploitation devrait s'appuyer sur une documentation complète et à jour des procédures relatives aux systèmes, concernant entre autres les exigences spécifiques relatives au traitement des données à caractère personnel.

91 Si tel n'est pas déjà le cas, les organisations devraient déterminer quels sont les systèmes informatiques existants qui traitent des données à caractère personnel, ainsi que les différents types de données traités (par exemple les données sensibles telles que les données relatives à la santé). Cela faciliterait la détection des risques associés au traitement de données à caractère personnel ainsi que la mise en place d'un système de contrôle interne adéquat pour garantir le respect de la législation relative à la protection des données.

92 L'évaluation des risques liés à l'exploitation des systèmes devrait être régulièrement examinée et mise à jour. Intégrer ce contrôle aux tâches régulières de gestion des risques de l'organisation qui exploite le système s'avère efficace.

R15: Le responsable du traitement devrait enregistrer auprès du délégué à la protection des données de l'institution tout traitement de données à caractère personnel effectué par l'intermédiaire d'une base de données ou d'un système informatique[41].

[41] Cette notification doit être conforme aux dispositions de l'article 25 du règlement (CE) nº 45/2001.

93 Les déclarations de confidentialité devraient être examinées régulièrement en cas de changement ou de services supplémentaires entraînant le traitement de données à caractère personnel.

R16: La durée de conservation maximale des données sur un support de stockage devrait être déterminée de manière à respecter les exigences contractuelles, légales et réglementaires. La durée de conservation peut varier en fonction de la finalité de la conservation[42].

5.6.1. Information des personnes concernées et transparence

94 Au minimum, l'institution est tenue d'informer l'utilisateur d'un système informatique des éléments suivants relatifs à l'opération de traitement:

a. l'identité de l'institution et de toute autre institution ou entité partageant la responsabilité du traitement des données et la méthode de contact de l'institution en cas de question ou de plainte;

b. les données à caractère personnel traitées;

c. les raisons (finalités) de la collecte et du traitement ultérieur des données par l'institution;

d. les destinataires ou les catégories de destinataires des données à caractère personnel, accompagnés de la description des services ou des catégories de membres du personnel ayant accès aux données;

e. les transferts à d'autres institutions ou entités et les raisons de ces transferts;

f. l'indication claire des informations obligatoires et facultatives dans la déclaration de confidentialité, même si un formulaire en ligne existe et indique les champs obligatoires et les champs facultatifs.

95 Les informations communiquées aux personnes concernées devraient être:

a. facilement et directement accessibles depuis la page d'accueil et toutes les autres pages utilisées pour collecter et traiter les données à caractère personnel;

b. formulées dans un langage simple et clair; et

c. clairement distinctes des autres informations juridiques et contractuelles.

96 Les institutions devraient permettre aux personnes handicapées[43] de comprendre pleinement leurs droits, en leur qualité de personnes concernées, et de les exercer

[42] Un système de sauvegarde disposera de différents contrôles d'accès et sera donc exposé à d'autres risques par rapport à un système opérationnel classique.

[43] En ce qui concerne les services internet, consulter par exemple cette page: http://www.w3.org/WAI/intro/accessibility.php.

efficacement si des données à caractère personnel sont traitées par l'intermédiaire de services informatiques.

R17: Les institutions devraient rédiger des avis d'information appropriés concernant les opérations de traitement et les rendre accessibles aux personnes concernées en recourant à différents moyens d'information.

97 Le moyen d'information approprié dépend de la nature du système informatique et des interactions entre les personnes concernées et l'institution. Si les personnes ont directement accès au système pendant le traitement des données (par exemple les systèmes de gestion internes pour le personnel ou les services internet pour les parties prenantes externes), le système devrait proposer la fonctionnalité d'information concernant le traitement dans l'interface utilisateur.

98 Lorsque les personnes concernées ne peuvent pas directement interagir avec les systèmes informatiques, les procédures organisationnelles doivent être conçues de manière à ce que les informations soient données au bon moment (par exemple lorsque les données sont collectées au moyen d'un formulaire, les informations peuvent être communiquées sur ce formulaire ou par l'intermédiaire d'un pointeur vers une source d'informations).

99 Les institutions doivent également être en mesure de communiquer les informations utiles sur demande, par l'intermédiaire d'une adresse électronique de contact ou d'un site internet dédié, et de répondre à de telles demandes dans un délai raisonnable.

5.6.2. Gestion des accès[44]

100 Il convient de déterminer clairement qui est le propriétaire du système et, dès lors, à qui incombe la responsabilité de gérer les risques du système de manière régulière. Le propriétaire du système est également tenu de contrôler les accès en permanence et de manière appropriée, de gérer les autres mesures de réduction des risques et de veiller à ce que les incidents de sécurité informatique et l'élimination des systèmes informatiques soient correctement gérés.

R18: Des procédures de gestion des comptes d'utilisateurs devraient être conçues et mises en place, ainsi que des procédures d'approbation relatives, entre autres, à l'octroi de droits d'accès à un système par le propriétaire de celui-ci.

101 L'équipe de gestion devrait régulièrement revoir les procédures d'accès et vérifier qu'elles sont bien appliquées.

[44] Voir également COBIT 5, le cadre de référence pour entreprises en matière de gouvernance et de gestion des technologies de l'information d'entreprise, pour en savoir plus sur les mesures de contrôle nécessaires.

102 L'accès aux données à caractère personnel devrait généralement être accordé selon le principe du privilège minimal, c'est-à-dire que seuls les droits d'accès nécessaires à l'exercice d'une fonction devraient être accordés aux utilisateurs et aux administrateurs.

5.6.3. Gestion des modifications

103 Des mesures de contrôle devraient être mises en place pour limiter l'accès aux composants du système et prévenir les modifications non autorisées.

> R19: Des procédures formelles de gestion des modifications devraient être créées et appliquées pour gérer de manière cohérente toutes les demandes de modification d'un système informatique.

104 Il est également recommandé de mettre en place des procédures de gestion des modifications pour les prestataires de services sous contrat (services de développement de systèmes ou d'applications, par exemple).

105 En cas de modification de la finalité du traitement des données à caractère personnel, les personnes concernées devraient en être informées et le fondement juridique de la nouvelle finalité devrait être déterminé. Les exigences en matière de protection des données devraient être analysées en concertation avec le DPD ou la personne occupant un poste équivalent.

5.6.4. Contrôle de la sécurité

> R20: L'accès aux fichiers contenant des données à caractère personnel devrait être surveillé en permanence.

> *Exemple: en cas de bogues dans l'exploitation du système, il convient d'éviter d'utiliser des données à caractère personnel réelles pour le débogage du code. En tout état de cause, si nécessaire, une autorisation du responsable du traitement des données doit être obtenue et tant le processus d'autorisation que les actions de débogage doivent être enregistrés et vérifiables. Le volume de données à caractère personnel utilisé pour les essais devrait d'une façon ou d'une autre être réduit au minimum et une politique stricte du «besoin d'en connaître» devrait être appliquée.*

106 Les institutions devraient s'assurer que leurs systèmes informatiques sont protégés grâce à des technologies de sécurité adéquates, que les mesures de réduction des risques définies lors de l'évaluation des risques pour la sécurité sont appliquées et que celles-ci sont toujours à jour, de manière à pouvoir faire face à n'importe quelle nouvelle menace.

107 Les systèmes d'information devraient générer les pistes d'audit nécessaires pour permettre de reconstruire la séquence des événements ou des modifications apportées au système informatique.

108 Il convient de garder à l'esprit que si la fonction de contrôle de la sécurité produit des journaux d'informations, ceux-ci doivent être examinés pour déterminer s'ils contiennent des données à caractère personnel, et donc s'ils doivent être pris en considération dans l'évaluation des risques. Par conséquent, la finalité du traitement et la durée de conservation doivent être clairement définies.

109 L'application des mesures de sécurité informatique doit être vérifiée et surveillée de manière proactive.

5.6.5. Échange de données

110 Il est important de détecter les diverses possibilités d'utilisation secondaire des données par des tiers ou d'échange des données avec ceux-ci. Les risques associés devraient être recensés car cela sera utile pour définir et concevoir des mesures de réduction des risques.

111 Pour obtenir des conseils pratiques et techniques sur les transferts de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions européennes, consulter le document d'orientation du CEPD[45] correspondant, ainsi que l'annexe 2 relative au traitement par des organisations externes et aux transferts de données à caractère personnel.

R21: Les données à caractère personnel ne devraient être transférées que par l'intermédiaire de connexions internet sécurisées. Le recours à des réseaux de confiance, à des moyens de transmission qui cryptent les données ou à des procédés équivalents permet d'y parvenir.

Exemple: lorsque des données à caractère personnel sont envoyées sur des réseaux publics comme l'internet, elles doivent être protégées contre les risques inhérents à ces réseaux, tels que le risque d'interception.

Les procédés de cryptage devraient être configurés correctement et accompagnés d'une gestion sécurisée des clés cryptographiques.

112 Les transferts manuels de données sur des supports physiques amovibles non protégés, tels que les clés USB, devraient être évités s'ils ne sont pas cryptés de manière sûre.

113 Il convient également d'éviter le transfert de données à caractère personnel vers un service infonuagique ou un espace de stockage en ligne s'il n'est pas accompagné d'une procédure d'autorisation adéquate. L'utilisation d'applications telles que Dropbox ou Google Drive devrait faire l'objet d'une gestion des risques appropriée[46].

---

[45] Document d'orientation du CEPD du 14 juillet 2014 sur le transfert de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions et organes de l'Union européenne.

[46] Attention: l'utilisation de ce type de service peut entraîner le transfert de données à caractère personnel à un pays tiers. Voir l'annexe 1 pour plus de détails.

Exemple: applications de messagerie électronique et de traitement de texte

Les logiciels de messagerie électronique et de traitement de texte sont utilisés dans toutes les institutions. Ces logiciels devraient être configurés de manière à ce que seules les données à caractère personnel nécessaires soient transférées, et il peut être nécessaire de vérifier, avant le transfert, que les fichiers ne contiennent pas de données à caractère personnel cachées.

114 Les responsables du traitement devraient mettre en place toutes les garanties nécessaires pour utiliser ces logiciels si des données à caractère personnel (relatives à la santé ou aux ressources humaines, par exemple) sont concernées.

R22: Les institutions qui transfèrent des données à caractère personnel sensibles[47] par courrier électronique devraient être conscientes des problèmes de protection des données inhérents à cette technologie, qui sont censés figurer dans l'évaluation des risques. Elles devraient en outre veiller à ce que ces transferts soient sécurisés, en utilisant par exemple un procédé de cryptage des fichiers ou un logiciel de messagerie qui crypte les données et les pièces jointes, ou en recourant à un réseau de confiance uniquement.

115 Des mesures supplémentaires devraient être envisagées afin d'interdire ou de prévenir la copie de données à caractère personnel stockées dans des applications vers des logiciels de traitement de texte personnels.

5.6.6. Élimination[48]

R23: Des procédures devraient être établies et mises en place pour garantir le respect des exigences de protection des données à caractère personnel lorsque les logiciels et équipements informatiques concernés sont éliminés ou transférés vers un autre environnement.

116 Si un système informatique devient obsolète, s'il est transféré ou s'il n'est plus utilisé, il convient de faire particulièrement attention à toute possibilité de divulgation non autorisée de données à caractère personnel.

117 Les durées de conservation convenues devraient être respectées lorsqu'un système informatique est éliminé.

118 L'accès à des systèmes obsolètes contenant des données à caractère personnel devrait être supprimé lorsque cet accès n'est plus nécessaire ou justifié.

[47] Techniquement parlant, tous les courriels contiennent des données à caractère personnel. Cette recommandation porte donc sur les données à caractère personnel supplémentaires contenues dans le message ou son objet.

[48] Voir également COBIT 5, le cadre de référence pour entreprises en matière de gouvernance et de gestion des technologies de l'information d'entreprise, pour en savoir plus sur les mesures de contrôle nécessaires.

119 Des procédures et des instructions devraient être mises en place en ce qui concerne la suppression des fichiers électroniques contenant des données à caractère personnel, ainsi que l'élimination des équipements informatiques en toute sécurité (supports de stockage, par exemple).

5.7. Procédures horizontales

5.7.1. Marchés publics et externalisation

120 Lorsque le développement d'un système informatique est programmé, il est décidé d'externaliser certaines tâches ou d'acheter des logiciels standard pour ce système. Une fois cette décision prise, une procédure de passation de marché est lancée.

R24: Le cahier des charges et les autres dispositions contractuelles devraient inclure des mesures de sécurité techniques et organisationnelles que le contractant devra respecter afin de garantir la protection des données à caractère personnel traitées, par exemple au cours de la phase de test.

121 Le recours à des clauses contractuelles modèles spécifiques relatives aux exigences de protection des données peut s'avérer utile à cet égard. Les données à caractère personnel traitées en relation avec la passation de marché et les procédures de sélection associées devraient être protégées conformément aux règles de protection des données[49].

122 Le DPD ou le CPD devraient participer à la procédure de passation de marché et y apporter leurs connaissances.

123 S'il est décidé d'externaliser le système informatique, le développement de celui-ci ou d'autres aspects du processus, l'équipe de gestion informatique devrait examiner les risques supplémentaires qui en découlent et les limites à la réduction de ces risques. En sa qualité de responsable du traitement, l'équipe de gestion informatique restera responsable même en cas d'externalisation et elle devra s'assurer que toutes les recommandations données sont appliquées autant que possible par le contractant concerné[50].

124 Alors qu'en vertu du RGPD (article 25), l'obligation contraignante de respecter les principes de protection des données dès la conception et de protection des données par défaut ne s'applique qu'aux responsables du traitement et ne s'applique pas directement aux fabricants de produits et prestataires de produits et de services standard, le considérant 78 dudit RGPD indique clairement que ces derniers devraient être incités à prendre en compte les principes de protection des données lors de l'élaboration et de la conception de leurs produits ou services. Selon ce même considérant, «*[l]es principes*

[49] Lignes directrices du CEPD concernant le traitement de données à caractère personnel dans le cadre des marchés publics, des subventions ainsi que de la sélection d'experts et du recours à ceux-ci.

[50] Pour en savoir plus sur l'externalisation, consulter l'annexe 1.

de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics». Les institutions européennes devraient s'assurer que leurs procédures de passation de marché pour les solutions informatiques sont établies en conséquence.

5.7.2. Gestion de projet

125 La gestion de projet consiste à appliquer des connaissances, des compétences, des outils et des techniques aux activités liées à un projet en vue de satisfaire aux spécifications de celui-ci[51].

5.7.2.1. Rôles et responsabilités

126 Le responsable de la protection des données (le DPD ou le CPD, par exemple) devrait participer à tout nouveau projet informatique dans le cadre duquel des données à caractère personnel sont traitées à tous les stades, ainsi qu'à toute initiative de recensement des bases de données ou des applications existantes qui traitent des données à caractère personnel. Il est conseillé de le consulter pour qu'il explique les exigences de protection des données et qu'il aide à vérifier que ces exigences ont été correctement prises en compte et appliquées efficacement dans le système, de manière à respecter la législation en matière de protection des données.

127 Il devrait également être consulté lors de la phase de démarrage d'un projet, au moment de déterminer si les données traitées par le système informatique sont à caractère personnel ou non.

128 De plus, son aide est essentielle lors du recensement et de l'évaluation des risques liés au traitement de données à caractère personnel.

R25: Le chef de projet d'un projet informatique en phase de développement ou le propriétaire du système devraient veiller à une bonne communication avec le responsable de la protection des données (le DPD ou le CPD).

129 Le chef de projet devrait également s'assurer que les exigences en matière de protection des données formulées par le responsable de la protection des données sont correctement analysées et appliquées dans le système. Ces exigences sont recueillies au lancement d'un projet (phase de démarrage et d'élaboration).

5.7.2.2. Formation aux exigences en matière de protection des données

130 Le chef de projet, l'équipe de projet (y compris l'équipe de développement) et le personnel en charge de l'exploitation et de la maintenance devraient suivre une formation aux règles de protection des données applicables organisée avec le DPD, ou être en mesure d'acquérir les connaissances demandées par d'autres moyens

[51] Définition donnée par le PMI (Project Management Institute).

équivalents. Ces personnes devraient également être au fait des technologies renforçant la protection de la vie privée et adopter une stratégie de prise en compte du respect de la vie privée dès la conception.

5.8. Logiciels standard

131 Les logiciels standard peuvent être achetés sur le marché.

132 Le cycle de vie complet de ces logiciels devrait être examiné: spécifications, sélection du produit approprié, installation et personnalisation, test, mise en production, gestion des licences et élimination.

133 La mise en service d'un logiciel standard devrait passer par les phases suivantes:

a. Planification: avant de choisir le logiciel standard, une liste des spécifications devrait être établie. À partir de cette liste, le logiciel peut être sélectionné de manière objective et transparente. Lors de cette phase, si les logiciels à sélectionner sont plus complexes, il est préférable de faire aussi appel au responsable des achats. Voir les sections 5.1 et 5.2, ainsi que les recommandations R6, R7, R8, R9 et R10.

b. Acquisition: la liste des spécifications établie permet de vérifier quel produit sur le marché propose les fonctionnalités les plus appropriées. Voir la section 5.7.1, l'annexe 1 et la recommandation R24.

c. Mise en place et test: il est nécessaire de tester les fonctionnalités spécifiées dans la documentation du logiciel standard. Voir les sections 5.4 et 5.5, ainsi que les recommandations R12, R13 et R14.

d. Personnalisation: d'une manière générale, le logiciel devra être personnalisé en fonction des besoins et des obligations juridiques de l'institution.

e. Installation: une gestion des licences et un contrôle de version efficaces sont nécessaires pour le logiciel standard.

f. Exploitation et maintenance: les procédures et règles définies au cours de l'installation doivent être maintenues et régulièrement revues. Voir les sections 5.6, 5.6.2, 5.6.3, 5.6.4, 5.6.5, ainsi que les recommandations R15, R16, R17, R18, R19, R20, R21 et R22.

g. Élimination: l'élimination en bonne et due forme d'un logiciel standard nécessite très souvent un travail complexe et considérable. Voir la section 5.6.6 et la recommandation R23.

6. LE MODÈLE DES TROIS LIGNES DE MAÎTRISE

134 Pour améliorer la surveillance d'une organisation, il existe un modèle mondialement reconnu, appelé «les trois lignes de maîtrise»[52]. Ce modèle peut également être utilisé comme référence en matière de protection des données, afin d'établir un cadre de gouvernance adéquat et de renforcer les responsabilités au sein de l'organisation.

135 Les trois lignes de maîtrise du modèle sont:

1. les managers,
2. les fonctions de gestion des risques et de conformité,
3. l'audit interne.

136 D'après ce modèle, les membres de la direction «donnent le ton» dans l'organisation et devraient insister sur l'importance de la protection des données à caractère personnel auprès de toutes les parties prenantes susceptibles d'interagir avec ces données. Ils sont particulièrement responsables de la protection des données et devraient également désigner un responsable en la matière.

137 Pour prouver que les règles de protection des données sont respectées et vérifier l'efficacité des mesures appliquées, l'équipe de gestion opérationnelle (les managers) définit les procédures appropriées ainsi que les rôles et les responsabilités, et met en place des activités de contrôle de ces procédures. Tous ces éléments font partie du système de contrôle interne d'une organisation. Les systèmes de contrôle interne devraient être conçus de manière à permettre à une institution d'atteindre ses objectifs[53].

138 Les contrôles internes peuvent être composés, entre autres, de politiques, de procédures, de garanties techniques et organisationnelles, d'analyses d'impact sur la protection des données, de codes de conduite et de certifications en matière de sécurité et de respect de la vie privée.

139 Les fonctions de conformité d'une organisation surveillent si les contrôles respectent les règles de protection des données concernées, tandis que les fonctions d'audit donnent aux membres de la direction une assurance indépendante concernant l'efficacité et l'efficience de ces contrôles.

140 Lors de la création d'un plan de travail pour l'audit interne, il est recommandé de veiller à ce que ce plan porte également sur les procédures et les fonctions de l'institution qui sont liées au traitement de données à caractère personnel et aux responsabilités en la matière.

---

[52] IIA Position Paper; the Three Lines of Defense in Effective Risk Management and Control, Altamonte Springs, FL: The Institute of Internal Auditors Inc., janvier 2013.

[53] Le contrôle interne est largement défini dans le règlement financier (article 32, paragraphe 2). Cette définition reflète fidèlement la définition standard du contrôle interne adoptée par l'organisme COSO.

141 Un tel audit permettrait d'évaluer l'adéquation et l'efficacité du système de contrôle interne pour minimiser le risque d'infraction aux règles de protection des données.

R26: Les auditeurs internes devraient participer à l'évaluation du système de contrôle interne mis en place afin de garantir son adéquation avec les règles de protection des données.

ANNEXES

Annexe 1: Traitement par des organisations externes et transferts de données à caractère personnel

Considérations générales

142 Les institutions européennes doivent évaluer les risques liés à la protection des données lorsqu'un service informatique est presté par un tiers et examiner la fiabilité de ce dernier en ce qui concerne la protection des données et les risques liés au renseignement.

143 Les données à caractère personnel collectées par les institutions européennes sont susceptibles d'être traitées par des organisations externes lorsqu'une institution a recours aux services d'un contractant ou d'une autre organisation externe pour effectuer certaines tâches. Cette organisation externe agit donc au nom de l'institution, en qualité de sous-traitant, et l'article 23 du règlement s'applique dès lors.

144 Toutefois, si l'organisation externe traite les données à caractère personnel collectées par une institution européenne à ses propres fins, elle sera également considérée comme responsable du traitement, à qui les données sont transférées ou mises à disposition. Les règles énoncées aux articles 7, 8 et 9 du règlement s'appliqueront à de tels transferts de données à caractère personnel[54].

145 Le personnel de l'organisation externe devrait être assujetti au mémorandum d'entente sur le contrôle de sécurité, afin de s'assurer qu'il est en mesure d'évaluer correctement les données à caractère personnel.

146 En vertu du règlement, le traitement par une organisation externe doit avoir des motifs légitimes et s'accompagner de garanties spécifiques. L'institution doit déterminer le rôle de l'organisation externe qui participera éventuellement au traitement de données à

[54] Un transfert de données à caractère personnel est normalement composé des éléments suivants: communication, puis divulgation ou mise à disposition, par un autre moyen, de données à caractère personnel que l'expéditeur soumis au règlement effectue en sachant que le destinataire aura accès à ces données ou dans l'intention qu'il y ait accès. Ces éléments s'appliquent aux transferts au sein des institutions ou organes de l'Union européenne ou entre ces institutions ou organes (article 7), aux transferts aux destinataires soumis à la directive 95/46/CE/RGPD (article 8) et aux transferts vers des pays tiers et des organisations internationales (article 9). Le terme désigne à la fois les transferts délibérés et les accès autorisés aux données par les destinataires. Les conditions de connaissance et d'intention ne s'appliquent pas aux cas d'accès illégaux (piratage, par exemple). Voir la section 3.1 du document d'orientation du CEPD sur les transferts à des pays tiers.

caractère personnel. Il convient de faire preuve d'une prudence particulière en cas de transfert de données à caractère personnel vers des pays extérieurs à l'Union européenne ou à l'Espace économique européen et vers des organisations internationales.

147 Les règles énoncées à l'article 9 du règlement s'appliqueront lorsque des données sont mises à la disposition d'une organisation externe située en dehors de l'Union, que le destinataire agisse ou non en qualité de sous-traitant ou de responsable du traitement supplémentaire. Pour obtenir plus d'informations sur les transferts de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions européennes, voir également le document d'orientation du CEPD correspondant[55].

Organisation externe agissant en qualité de sous-traitant

148 Si l'organisation externe agit en qualité de sous-traitant d'une institution européenne, l'article 23 du règlement relatif aux relations entre le responsable du traitement et le sous-traitant et aux obligations qui incombent à ce dernier s'applique alors[56].

149 Si le sous-traitant est une organisation externe située en dehors de l'UE, l'article 9 du règlement s'applique en plus des dispositions de l'article 23. Lorsque des services informatiques sont prestés par une organisation située en dehors de l'Union européenne, il est important de prendre en considération les dispositions de l'article 9 au moment de choisir le sous-traitant et d'évaluer le niveau de protection des données à caractère personnel qu'il offre.

150 L'institution doit s'assurer que le sous-traitant externe n'agira qu'en son nom et selon ses instructions, conformément à l'article 23 du règlement. Tout cela doit être mis par écrit dans un contrat passé entre l'institution et le sous-traitant, assorti de dispositions claires en matière de protection des données, portant entre autres sur les mesures de sécurité et les mesures techniques et organisationnelles que le sous-traitant doit mettre en place conformément aux articles 21 et 22 du règlement.

151 L'institution est tenue d'informer le sous-traitant des exigences et des mesures en matière de sécurité définies à la suite d'une évaluation des risques informatiques. Elle doit ensuite vérifier que le sous-traitant a mis en place ces mesures.

Organisation externe agissant en qualité de responsable du traitement

152 En principe, les institutions devraient éviter de donner à des entités externes la possibilité de devenir responsables du traitement de données à caractère personnel, à moins que cela ne soit nécessaire à la réalisation de leurs objectifs institutionnels, par

[55] Document d'orientation du 14 juillet 2014 sur le transfert de données à caractère personnel à des pays tiers et des organisations internationales par les institutions et organes de l'Union européenne.

[56] Les articles 7 et 8 du règlement ne s'appliquent pas lorsque des institutions européennes mettent des données à la disposition d'un sous-traitant situé dans un pays de l'Union européenne, étant donné qu'il travaille directement sous la responsabilité du responsable du traitement.

exemple lorsqu'une institution européenne coopère avec une organisation internationale dans le domaine humanitaire ou autre.

153 Les articles 7, 8 et 9 du règlement régissent les transferts de données à caractère personnel. Les institutions ne peuvent transférer des données à caractère personnel que lorsqu'elles sont nécessaires et les destinataires des données transférées en vertu des articles 7, 8 et 9 du règlement doivent traiter ces données uniquement aux fins auxquelles elles ont été transmises.

154 Si une organisation externe agit en qualité de responsable du traitement, c'est-à-dire à ses propres fins, elle devra assumer toutes les responsabilités liées à cette qualité, y compris les obligations de ne transférer des données à caractère personnel qu'à des destinataires ayant un niveau de protection adéquat et de transférer ces données uniquement dans le but d'effectuer les tâches du responsable du traitement.

155 Dans un souci de transparence, les institutions devraient communiquer aux personnes concernées les informations suivantes concernant leurs services informatiques:

a. quelles sont les opérations de traitement effectuées par l'organisation en qualité de sous-traitant et celles effectuées en qualité de responsable du traitement;

b. toute information utile concernant les pratiques de protection des données de l'organisation tierce en sa qualité de responsable du traitement.

Annexe 2: Recommandations en matière de protection des données dans les différentes phases du cycle de vie d'un système informatique

Phases du cycle de vie d'un système informatique	Procédures et sous-procédures	Recommandations	Recommandation générale
Démarrage		**R6**En premier lieu, il convient de déterminer si les données traitées par le système informatique concerné sont à caractère personnel ou non, ou si elles pourraient le devenir à la suite d'un tel traitement.	**Les principes généralement reconnus de protection des données devraient être respectés dans toutes les phases du cycle de vie d'un système informatique (voir section 4.1).**
		R7 Les exigences élevées en matière de protection des données devraient être incluses dans une charte de projet, étant donné que ce document comporte le cahier des charges et les spécifications de haut niveau, et qu'il résulte de la phase de démarrage.	
Élaboration	Collecte des exigences	**R8** Les exigences de protection des données devraient être recueillies auprès des parties prenantes et documentées au cours de la phase de spécification du système informatique.	
	Conception	**R9** Des mesures de sécurité supplémentaires, telles que le cryptage et les contrôles d'accès multiniveaux, devraient être mises en place pour réduire les risques élevés liés au traitement informatique de données (à caractère personnel) particulièrement sensibles relatives, par exemple, à la santé physique ou mentale, à l'origine raciale ou ethnique, aux opinions politiques, aux croyances religieuses ou aux décisions pénales.	
		R10 Des fonctionnalités adéquates devraient être intégrées au système informatique afin de pouvoir gérer correctement les durées de conservation et exécuter les actions nécessaires par la suite, par exemple l'anonymisation ou la suppression des données.	
Construction	Développement	**R11** Il est important d'établir une entente commune entre l'équipe de développement et les parties prenantes. Cette équipe devrait être au fait de la législation et des règles relatives à la protection des données ou suivre une formation en la matière avant que ne commence la phase de développement. Pour s'en assurer, il peut s'avérer utile d'organiser avec le DPD une formation des membres actuels et nouveaux de l'équipe de développement, ou de mettre en place des initiatives équivalentes.	
	Test	**R12** Les procédures et les instructions de test devraient être élaborées de manière à garantir l'adéquation avec les exigences de protection des données.	
		R13 Il est préférable d'éviter l'échantillonnage de vraies données à caractère personnel lors d'une simulation d'environnement réel.	

Phases du cycle de vie d'un système informatique	Procédures et sous-procédures	Recommandations	Recommandation générale
Transition et déploiement		**R14** Les utilisateurs finaux, les administrateurs du système et le personnel de maintenance devraient connaître les règles de protection des données.	
Exploitation et maintenance		**R15 Le responsable du traitement devrait enregistrer auprès du délégué à la protection des données de l'institution tout traitement de données à caractère personnel effectué par l'intermédiaire d'une base de données ou d'un système informatique.**	
		R16 La durée de conservation maximale des données sur un support de stockage devrait être déterminée de manière à respecter les obligations contractuelles, légales et réglementaires. La durée de conservation peut varier en fonction de la finalité de la conservation.	
	Information des personnes concernées et transparence	**R17** Les institutions devraient rédiger des avis d'information appropriés concernant les opérations de traitement et les rendre accessibles aux personnes concernées en recourant à différents moyens d'information.	
	Gestion des accès	**R18** Des procédures de gestion des comptes d'utilisateurs devraient être établies et mises en œuvre, ainsi que des procédures d'approbation relatives, entre autres, à l'octroi de droits d'accès à un système par le propriétaire de celui-ci.	
	Gestion des modifications	**R19** Des procédures formelles de gestion des modifications devraient être créées et appliquées pour gérer de manière cohérente toutes les demandes de modification d'un système informatique.	
	Contrôle de la sécurité	**R20** L'accès aux fichiers contenant des données à caractère personnel devrait être surveillé en permanence.	
	Échange de données	**R21** Les données à caractère personnel ne devraient être transférées que par l'intermédiaire de connexions internet sécurisées. Le recours à des réseaux de confiance, à des moyens de transmission qui cryptent les données ou à des procédés équivalents permet d'y parvenir.	
		R22 Les institutions qui transfèrent des données à caractère personnel sensibles par courrier électronique devraient être conscientes des problèmes de protection des données inhérents à cette technologie, qui sont censés figurer dans l'évaluation des risques. Elles devraient en outre veiller à ce que ces transferts soient sécurisés, en utilisant, par exemple, un procédé de cryptage des fichiers ou un logiciel de messagerie qui crypte les données et les pièces jointes, ou en recourant à un réseau de confiance uniquement.	

Phases du cycle de vie d'un système informatique	Procédures et sous-procédures	Recommandations	Recommandation générale
	Élimination	**R23** Des procédures devraient être établies et mises en œuvre pour garantir le respect des exigences de protection des données à caractère personnel lorsque les logiciels et équipements informatiques concernés sont éliminés ou transférés vers un autre environnement.	
Procédures horizontales	Marchés publics	**R24** Le cahier des charges et les autres dispositions contractuelles devraient inclure des mesures de sécurité techniques et organisationnelles que le contractant devra respecter afin de garantir la protection des données à caractère personnel traitées, par exemple, au cours de la phase de test.	
	Gestion de projet	**R25** Le chef de projet d'un projet informatique en phase de développement ou le propriétaire du système devraient veiller à une bonne communication avec le responsable de la protection des données (le DPD ou le CPD).	
	Gouvernance	**R1** Il est extrêmement important que les principes de protection des données soient explicitement soutenus par la direction d'une organisation.	
		R2 Les membres de la direction, s'ils remplissent la fonction de responsable du traitement, doivent rendre des comptes en matière de protection des données. S'ils ne remplissent pas eux-mêmes la fonction de responsable du traitement, les membres de la direction sont malgré tout responsables de veiller au respect des règles de protection des données.	
		R3 Les membres de la direction devraient assumer la responsabilité de la protection des données et désigner un responsable en la matière (un délégué à la protection des données ou un coordinateur de la protection des données, par exemple), qu'ils chargeront d'appliquer les politiques de protection des données.	
		R4 L'ensemble du personnel devrait connaître les politiques et procédures existantes en matière de protection des données. Une formation d'intégration obligatoire, la distribution de documents d'information ou des formations périodiques sont des moyens d'y parvenir.	
		R5 Les politiques, les procédures ainsi que les responsabilités et les fonctions concernant la protection des données devraient être régulièrement surveillées et actualisées.	
		R26 Les auditeurs internes devraient participer à l'évaluation du système de contrôle interne mis en	

Phases du cycle de vie d'un système informatique	Procédures et sous-procédures	Recommandations	Recommandation générale
		place afin de garantir son adéquation avec les règles de protection des données.	