COMMISSION EUROPÉENNE

Bruxelles, le 25.1.2012
SEC(2012) 73 final

**DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION**

**RÉSUMÉ DE L'ANALYSE D'IMPACT**

***accompagnant les documents***

**Règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données).**
**et**
**Directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données**

{COM(2012) 10 final}
{COM(2012) 11 final}
{SEC(2102) 72 final}

**DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION**

**RÉSUMÉ DE L'ANALYSE D'IMPACT**

***accompagnant les documents***

**Règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données).**
**et**
**Directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données**

## 1. INTRODUCTION

Depuis l'adoption du cadre juridique actuel de l'UE en matière de protection des données, en 1995, la rapide évolution des technologies et de l'environnement des entreprises a créé de nouveaux enjeux pour la protection des données à caractère personnel. La collecte et le partage de données ont connu une augmentation spectaculaire. Les nouvelles technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus de personnes physiques rendent des informations les concernant accessibles à tout un chacun, où qu'il se trouve dans le monde, sans être pleinement conscientes des risques encourus.

Or l'instauration d'un climat de confiance dans l'environnement en ligne est essentielle au développement économique. En effet, s'ils n'ont pas totalement confiance, les consommateurs hésiteront à faire des achats en ligne et à recourir à de nouveaux services, y compris aux services administratifs en ligne. S'il n'y est pas remédié, ce manque de confiance continuera de ralentir l'innovation dans l'utilisation des nouvelles technologies, d'entraver la croissance économique et de priver le secteur public des avantages potentiels de la numérisation de ses services.

En outre, le traité de Lisbonne a créé, avec l'article 16 du TFUE, une nouvelle base juridique permettant d'adopter une approche modernisée et globale de la protection des données et de la libre circulation des données à caractère personnel, intégrant la coopération policière et judiciaire en matière pénale.

## 2. FORMULATION DU PROBLEME

L'analyse d'impact présente et analyse trois grands problèmes.

### 2.1. Problème n° 1: obstacles pour les entreprises et les autorités publiques dus à la fragmentation, à l'insécurité juridique et à une application non cohérente

Bien que la directive ait eu pour objectif d'assurer un niveau équivalent de protection des données dans toute l'Union européenne, des divergences considérables demeurent entre États membres en ce qui concerne les règles appliquées. Il peut ainsi arriver que les responsables du traitement des données soient confrontés à 27 législations et exigences nationales différentes dans l'Union. Il en résulte un environnement juridique fragmenté qui a fait naître une insécurité juridique et produit une protection inégale des personnes physiques. Cette situation génère des coûts inutiles et des **charges administratives** (se montant à **environ 3 milliards d'euros par an** dans le scénario de base) pour les entreprises et constitue un facteur de dissuasion pour celles, notamment les PME, qui exercent leurs activités sur le marché unique et qui souhaiteraient les étendre au-delà des frontières.

En outre, les ressources et les pouvoirs des autorités nationales chargées de la protection des données varient considérablement d'un État membre à l'autre. Dans certains cas, ces autorités ne sont dès lors pas en mesure de veiller de façon satisfaisante à la bonne application de la législation en vigueur. La coopération entre elles au niveau européen, dans le cadre du groupe consultatif existant (le groupe de travail «article 29»), ne conduit pas toujours à une application cohérente et doit donc également être améliorée.

### 2.2. Problème n° 2: difficulté pour les personnes physiques de maîtriser l'utilisation qui est faite de leurs données à caractère personnel

En raison de cette absence d'harmonisation des législations nationales sur la protection des données et des pouvoirs inégaux dont jouissent les autorités nationales chargées de cette protection, l'exercice par les personnes physiques de leurs droits en matière de protection des données est plus difficile dans certains États membres que dans d'autres, notamment dans l'environnement en ligne.

Les personnes physiques ne maîtrisent plus non plus l'utilisation qui est faite des données les concernant, à cause du volume considérable de données échangées chaque jour et parce que, souvent, ces personnes n'ont pas pleinement conscience du fait que leurs données sont collectées. Même si nombre d'Européens considèrent que la divulgation de données à caractère personnel fait de plus en plus partie de la vie moderne[1], 72 % des internautes en Europe s'inquiètent néanmoins du nombre de données à caractère personnel qu'ils sont invités à communiquer en ligne. De plus, une grande partie de ces utilisateurs ne savent pas comment faire valoir leurs droits en ligne.

[1] Voir Eurobaromètre spécial 359 (en anglais) – *Attitudes on Data Protection and Electronic Identity in the European Union*, juin 2011, p. 23.

### 2.3. Problème n° 3: lacunes et incohérences dans la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale

Le champ d'application de la directive, qui reposait sur une base juridique du marché intérieur, excluait expressément la coopération policière et judiciaire en matière pénale. La décision-cadre adoptée en 2008 afin de réglementer les traitements de données intervenant dans le cadre de la coopération policière et de la coopération judiciaire en matière pénale reflète les spécificités de la structure de l'UE «en piliers» antérieure au traité de Lisbonne et se caractérise par **un champ d'application limité et diverses autres lacunes**, qui ont souvent créé une insécurité juridique pour les personnes physiques et les services répressifs, ainsi que des difficultés pratiques de mise en œuvre. En outre, cette décision-cadre prévoit de nombreuses possibilités de déroger aux principes généraux de la protection des données au niveau national, et n'assure donc aucune harmonisation. Une telle approche risque non seulement de vider ces principes de leur contenu – et donc de porter atteinte au droit fondamental des personnes physiques à la protection de leurs données à caractère personnel dans ce domaine – mais également d'empêcher le bon échange des données à caractère personnel entre les autorités nationales compétentes.

## 3. ANALYSE DE SUBSIDIARITE ET DE PROPORTIONNALITE

À la lumière des problèmes décrits ci-dessus, l'analyse de subsidiarité indique qu'une action au niveau de l'Union est nécessaire pour les raisons suivantes:

- le droit à la protection des données à caractère personnel est énoncé à l'article 8 de la charte des droits fondamentaux. L'article 16 du TFUE est la base juridique nécessaire à l'adoption de dispositions de l'Union européenne en matière de protection des données;
- les données à caractère personnel peuvent être transférées de plus en plus rapidement au-delà des frontières nationales, que ce soit vers d'autres États membre de l'Union ou vers des pays tiers. En outre, le contrôle de la bonne application de la législation sur la protection des données pose des problèmes pratiques, et il conviendrait d'instaurer une coopération entre les États membres et leurs autorités, organisée au niveau de l'Union, afin d'assurer la cohérence nécessaire et un niveau élevé de protection au sein de l'Union;
- les États membres ne sont pas en mesure de résoudre seuls les problèmes posés par la situation actuelle, en particulier ceux dus à la fragmentation des législations nationales mettant en œuvre le cadre réglementaire de l'Union en matière de protection des données;
- bien que les États membres aient la possibilité d'adopter des politiques pour assurer le respect de ce droit, l'uniformité de ces politiques serait utopique en l'absence de règles communes au niveau de l'Union et des limitations seraient apportées aux flux transfrontières de données à caractère personnel.

**Les actions prévues sont proportionnées**, car elles relèvent des compétences de l'Union telles que définies par les traités, et elles sont nécessaires pour assurer une application uniforme de la législation de l'UE, permettant une protection effective et égale des droits fondamentaux des personnes physiques. Une action au niveau de l'Union constitue un gage essentiel de crédibilité à terme et permettra de maintenir un niveau élevé de protection des données à l'ère de la mondialisation, sans entraver la libre circulation des données. Pour que le marché intérieur fonctionne bien, la législation doit garantir des conditions uniformes aux opérateurs économiques.

## 4. OBJECTIFS

Les trois principaux **objectifs stratégiques** sont les suivants:

- **renforcer la dimension «marché intérieur» de la protection des données»** en atténuant la fragmentation, en renforçant la cohérence et **en simplifiant** l'environnement réglementaire, ce qui éliminerait les coûts inutiles et **réduirait la charge administrative**;

- **rendre l'exercice du droit fondamental à la protection des données plus effectif et donner aux personnes physiques la maîtrise de l'utilisation des données les concernant**;

- **améliorer la cohérence du cadre européen de la protection des données**, y compris dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, en tenant pleinement compte de l'entrée en vigueur du traité de Lisbonne.

## 5. OPTIONS

### 5.1. Option n° 1: mesures «douces»

Cette option consisterait principalement à établir **des communications interprétatives de la Commission** et à prévoir **des outils d'assistance technique et un financement,** ainsi qu'à **encourager la normalisation et l'autorégulation,** afin de renforcer la mise en œuvre pratique des règles existantes par les responsables du traitement des données et de sensibiliser les personnes physiques. La Commission proposerait **uniquement des modifications législatives très limitées** visant à préciser les notions utilisées dans la directive et à résoudre des questions spécifiques qui ne peuvent être traitées efficacement d'une autre manière. Cette option ne serait pertinente que pour les problèmes n$^{os}$ 1 et 2.

Ces changements législatifs limités introduiraient expressément les principes de transparence et de minimisation des données, de même qu'une base juridique pour les «règles d'entreprise contraignantes» applicables aux transferts internationaux.

### 5.2. Option n° 2: cadre juridique modernisé

La Commission présenterait **des propositions législatives destinées à poursuivre l'harmonisation des règles de fond**, à clarifier certaines dispositions et à éliminer les incohérences dues aux approches divergentes adoptées dans les États membres. Ces propositions offriraient une solution aux problèmes n$^{os}$ 1 et 2, car elles permettraient, d'une part, de **faciliter les flux de données à l'intérieur de l'Union et de l'UE vers les pays tiers** et, d'autre part, de **préciser et** de **renforcer les droits des personnes physiques** (par exemple le droit d'accès, le «droit à l'oubli numérique», des modalités plus claires pour le consentement et la notification des violations de données) **et d'accroître les obligations – et le «principe de responsabilité» - des responsables du traitement des données et des sous-traitants** [par exemple en instaurant, lorsque c'est pertinent, l'obligation de nommer des délégués à la protection des données (DPD) ou de réaliser des analyses d'impact relatives à la protection des données]. Cette option prévoit plus particulièrement de créer un «**guichet unique**» pour les responsables du traitement des données (c'est-à-dire une seule législation et

une seule autorité chargée de la protection des données). Les exigences en matière de notification générale seraient simplifiées (grâce à un système d'«enregistrement de base»). **En outre, les autorités chargées de la protection des données jouiraient d'une plus grande indépendance et disposeraient de pouvoirs harmonisés**. La coopération et l'assistance mutuelle entre les autorités chargées de la protection des données seraient renforcées, notamment grâce à un nouveau **«mécanisme de contrôle de la cohérence»** auquel participeraient à la fois un «comité européen de la protection des données» – qui serait à créer – et la Commission.

En ce qui concerne la protection des données dans le cadre de la coopération policière et judiciaire en matière pénale (problème n° 3), la Commission présenterait des propositions visant à remplacer la décision-cadre par **un nouvel instrument doté d'un champ d'application élargi** et elle comblerait **les principales lacunes**, pour, d'une part, renforcer les droits des personnes physiques et, d'autre part, faciliter la coopération entre les services répressifs, tout en tenant compte des spécificités de ce secteur.

### *5.3.* Option n° 3: réglementation détaillée au niveau de l'UE

Cette option inclurait la plupart des éléments de l'option n° 2, ainsi que **l'élaboration d'une législation de l'Union beaucoup plus détaillée**, y compris sur le plan sectoriel (par exemple, dans le secteur médical et des soins de santé), et **la mise en place au niveau de l'Union d'une structure centralisée de contrôle de l'application** (c'est-à-dire d'une autorité de l'UE chargée de la protection des données). Elle impliquerait en outre l'élimination des exigences de notification générale (à l'exception de la vérifications préalable pour les traitements à risques), la mise en place d'un système de certification à l'échelle de l'Union pour les processus et les produits conformes aux exigences en matière de protection des données, et la définition de sanctions pénales harmonisées au niveau de l'Union pour les infractions aux règles de protection des données. Le consentement serait défini comme étant le «fondement principal» du traitement des données.

En ce qui concerne la coopération policière et judiciaire en matière pénale, outre les mesures de fond prévues dans l'option n° 2, l'option n° 4 comprendrait l'établissement de règles détaillées régissant l'exercice du droit d'accès (toujours direct) des personnes physiques. Elle inclurait également **la modification des dispositions pertinentes de tous les instruments existants relevant de l'ancien troisième pilier**, afin de les aligner entièrement sur les nouvelles règles harmonisées et élargies.

## 6. ANALYSE D'IMPACT

### 6.1. Option n° 1: mesures «douces»

Les communications interprétatives de la Commission relatives aux dispositions de la directive ne seraient pas contraignantes et n'auraient, de ce fait, **qu'une incidence limitée sur la réduction de l'insécurité juridique et des coûts**. Une autorégulation accrue à l'échelle de l'Union pourrait apporter davantage de clarté juridique aux responsables du traitement des données dans certains secteurs, mais elle **ne suffirait pas** à garantir une application effective et cohérente des règles en l'absence d'un cadre juridique clair et harmonisé au niveau de l'Union.

**Des campagnes de sensibilisation aideraient** les personnes physiques à mieux connaître leurs droits en matière de protection des données et à mieux comprendre les moyens dont elles disposent pour les exercer dans la pratique. Cette mesure serait cependant **insuffisante** pour que les personnes physiques puissent faire valoir leurs droits lorsque ces derniers ne sont pas clairement définis par la loi. **Des éclaircissements de la législation** en ce qui concerne les notions de transparence, de minimisation des données, de niveau de protection adéquat et de règles d'entreprise contraignantes accroîtraient l'harmonisation et la sécurité juridique pour les personnes physiques et les entreprises.

En ce qui concerne **le contrôle de l'application de la législation**, les communications de la Commission ne suffiraient pas à vaincre la réticence des États membres à modifier leurs règles nationales pour conférer une plus grande indépendance et des pouvoirs harmonisés aux autorités chargées de la protection des données. Une coordination accrue par le groupe de travail «article 29» et des échanges entre les autorités chargées de la protection des données permettraient d'assurer une application plus cohérente; toutefois, **les divergences qui persisteraient entre les législations nationales et entre leurs interprétations limiteraient l'effet d'une amélioration de la coopération entre ces autorités**.

**L'incidence financière et économique attendue de cette option est limitée** et les problèmes recensés resteraient, pour la plupart, non résolus.

### 6.2. Option n° 2: cadre juridique modernisé

**L'insécurité juridique diminuerait sensiblement** pour les entreprises privées et les autorités publiques. Les dispositions problématiques seraient clarifiées et la cohérence serait améliorée grâce à la marge d'interprétation réduite et aux mesures d'exécution et/ou aux actes délégués adoptés par la Commission.

Le remplacement de la notification générale des activités de traitement de données par un **système d'«enregistrement» harmonisé** et simplifié, qui maintiendrait néanmoins les vérifications préalables pour les données sensibles et les traitements à risques, soulagerait les responsables du traitement des données d'une obligation actuellement exécutée de diverses manières. La responsabilité incombant aux responsables du traitement des données et aux sous-traitants serait renforcée en imposant, dans certains cas et avec des seuils précis et ciblés, la désignation de DPD et la réalisation d'analyses d'impact relatives à la protection des données, et le principe de la protection des données dès la conception serait posé, deux mesures qui permettront d'assurer et de démontrer plus facilement le respect des règles en vigueur.

**La clarification et la simplification de la réglementation par la définition d'une législation unique applicable dans toute l'Union et la mise en place d'un «guichet unique» pour la surveillance de la protection des données permettront de consolider le marché intérieur**, notamment en supprimant les différences entre les formalités administratives à remplir par les autorités chargées de la protection des données. Un **montant total** d'environ **2,3 milliards d'euros** par an pourra ainsi être **économisé**, uniquement en ce qui concerne la charge administrative.

**L'application de la législation deviendra également plus cohérente** grâce au renforcement et à l'harmonisation des pouvoirs des autorités chargées de la protection des données, à l'instauration d'un mécanisme solide de coopération et d'assistance mutuelle pour les cas qui

présentent une dimension européenne, et à l'harmonisation des infractions passibles de sanctions administratives.

**Une obligation de notifier les violations de données, harmonisée au niveau de l'Union européenne**, permettra de mieux protéger les personnes physiques, d'assurer la cohérence entre les secteurs et d'éviter les désavantages concurrentiels.

**Les droits des personnes concernées et la maîtrise des personnes physiques sur l'utilisation qui est faite de leurs données seraient considérablement renforcés** par la création de nouveaux droits et par l'amélioration et la clarification des droits existants. Les enfants feront l'objet de mesures spécifiques tenant compte de leur vulnérabilité. Les associations auront une plus grande latitude pour aider les personnes concernées à exercer leurs droits, y compris dans les actions en justice.

**L'application des principes généraux de la protection des données au domaine de la coopération policière et judiciaire en matière pénale** augmenterait la cohérence globale du cadre de protection des données de l'Union, tout en respectant les spécificités inhérentes au domaine répressif. Les droits des personnes physiques seraient notamment renforcés par l'extension du champ d'application de la protection des données dans ce domaine aux traitements «nationaux», par la fixation de conditions garantissant le droit d'accès et par la définition de règles plus strictes en matière de limitation de la finalité.

En ce qui concerne **l'incidence financière et économique**, l'obligation imposée aux opérateurs économiques plus importants (plus de 250 employés) de désigner des DPD **ne générera pas de coûts disproportionnés**, puisque des DPD existent déjà souvent dans ce type d'entreprises. Le coût de la mise en conformité représenterait un montant de 320 millions d'euros par an. Cette obligation s'appliquerait à un pourcentage minimal nécessaire des responsables du traitement des données, les PME en étant dispensées par principe, à moins que leurs activités de traitement de données ne comportent des risques significatifs en matière de protection des données. Les autorités et organismes publics seraient autorisés à désigner un seul DPD pour plusieurs entités (par exemple, pour plusieurs établissements, départements, services), compte tenu de leur structure organisationnelle.

La simplification des règles applicables aux transferts internationaux de données (par exemple, en étendant le champ d'application des «règles d'entreprise contraignantes») aurait également une incidence positive sur la compétitivité internationale des entreprises de l'Union.

Le renforcement de l'indépendance et des pouvoirs des autorités chargées de la protection des données, ainsi que l'obligation faite aux États membres de leur fournir des ressources suffisantes, entraîneraient des coûts supplémentaires pour les autorités publiques qui ne disposent pas actuellement des compétences nécessaires et de ressources adéquates.

Le nouveau mécanisme de coopération et d'assistance mutuelle entre les autorités chargées de la protection des données générerait lui aussi un coût supplémentaire pour ces dernières et pour le CEPD. Par exemple, pour les tâches supplémentaires confiées au CEPD, qui assurerait le secrétariat du comité européen de la protection des données remplaçant le groupe de travail «article 29», et notamment pour sa participation au mécanisme de contrôle de la cohérence, le budget actuel du CEPD devra probablement être augmenté de 3 millions d'euros par an en moyenne pour les six premières années, montant qui comprend l'engagement de 10 personnes supplémentaires.

### 6.3. Option n° 3: réglementation détaillée au niveau de l'UE

Ajouter des règles juridiques plus précises, y compris de nature sectorielle, dépassant les mesures prévues dans l'option n° 2 permettrait d'obtenir **une réduction maximale des disparités entre les États membres**. Toutefois, ces derniers pourraient ne pas disposer d'une marge de manœuvre suffisante pour tenir compte des spécificités nationales

La suppression totale des notifications, sauf en cas de contrôles préalables, simplifierait considérablement l'environnement réglementaire et réduirait la charge administrative.

La mise en place d'une agence de l'UE chargée de la protection des données permettrait d'**assurer une application beaucoup plus cohérente de la législation** et de remédier aux incohérences dans les cas qui présentent une dimension européenne manifeste, mais les pouvoirs d'une telle agence de l'Union pourraient aller trop loin au regard du droit de l'Union. Cette option serait toutefois très coûteuse pour le budget de l'Union. Des sanctions pénales harmonisées permettraient également d'appliquer la législation d'une façon plus cohérente, mais elles se heurteraient, elles aussi, à une forte opposition des États membres.

Les droits des personnes concernées, y compris ceux des enfants, seraient encore renforcés, par exemple en étendant la définition des données sensibles aux données relatives aux enfants, aux données biométriques et aux données financières. La création d'un droit aux «actions collectives» pourrait favoriser le plein exercice des droits par la voie judiciaire. L'harmonisation du niveau des sanctions, y compris des sanctions pénales, à l'échelle de l'Union devrait permettre de renforcer encore les droits individuels.

Apporter des modifications explicites à tous les instruments, pour étendre les règles générales de protection des données au domaine de la coopération policière et judiciaire en matière pénale, favoriserait la cohérence des règles dans ce domaine et renforcerait les droits des personnes physiques. Une approche aussi radicale se heurterait cependant à la résistance des États membres et serait difficile à mettre en œuvre sur le plan politique.

## 7. COMPARAISON DES OPTIONS

En ce qui concerne l'***option n° 1***, les coûts de mise en conformité et les coûts administratifs seraient peu élevés, notamment pour les responsables du traitement des données, puisque la plupart des coûts supplémentaires incomberaient aux autorités publiques des États membres et de l'UE. Dans le même temps, elle n'aurait qu'**un impact positif limité sur les problèmes recensés et sur la réalisation des objectifs stratégiques**.

Du point de vue de la faisabilité politique, bien que les propositions ne prêtent pas à controverse, cette option rencontrerait vraisemblablement la résistance des parties prenantes en raison de sa portée restreinte et de son incidence limitée sur les problèmes à résoudre, et serait considérée comme manquant d'ambition.

L'***option n° 2*** diminuera **sensiblement la fragmentation et l'insécurité juridique**. Elle devrait contribuer dans une beaucoup plus large mesure à la résolution des problèmes constatés et à la réalisation des objectifs stratégiques. Le bilan des **coûts administratifs et de mise en conformité associés à cette option devrait être raisonnable, compte tenu des avantages retirés et des quelque 2,3 milliards d'euros économisés chaque année au niveau de la charge administrative, un aspect qui sera essentiel pour les entreprises**. Cette option devrait garantir dans l'ensemble une application plus efficace et plus cohérente

de la législation. La suppression des notifications, pour passer à un «système d'enregistrement de base» beaucoup plus simple, permettrait également de simplifier l'environnement réglementaire et de réduire la charge administrative.

Quant à son acceptation par les parties intéressées, cette option serait accueillie favorablement par une grande partie des opérateurs économiques et des autorités publiques, car elle leur permettrait de réduire globalement leurs coûts de mise en conformité, notamment ceux liés à l'actuel régime fragmenté. Les acteurs de la protection des données, et en particulier les autorités qui en sont chargées, se féliciteraient du renforcement des droits dans ce domaine. En ce qui concerne le troisième objectif général, cette option contribuerait à la réalisation des objectifs consistant à assurer **une plus grande cohérence des règles de protection des données dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale**, en abrogeant et en «lisbonisant» la décision-cadre, comblant ainsi ses lacunes, notamment en étendant son champ d'application aux traitements «nationaux».

L'***option n° 3*** comprend la plupart des mesures prévues dans l'option n° 2, mais va beaucoup plus loin sur plusieurs plans. Elle aurait donc **une incidence positive marquée, tant en termes de réduction des coûts liés à la fragmentation juridique que d'amélioration des droits des personnes physiques**. En outre, elle permettrait de maximiser la cohérence des règles de protection des données relevant de l'ancien troisième pilier, et de relever les normes de protection des données dans ce contexte. Toutefois, certaines des actions prévues dans cette option **entraînent des coûts de mise en conformité excessifs ou sont susceptibles de se heurter à une forte opposition de la part des parties prenantes**. De plus, la modification simultanée de tous les instruments relevant de l'ancien troisième pilier serait très compliquée à réaliser et soulèverait des controverses sur le plan politique.

**Option privilégiée**

L'***option privilégiée*** consiste en l'option n° 2 combinée à:

– la suppression des obligations de notification prévue dans l'option n° 3, et

– certaines des mesures «douces» prévues dans l'option n° 1, à savoir l'encouragement des technologies renforçant la protection de la vie privée et des régimes de certification, et des campagnes de sensibilisation.

L'option privilégiée est la plus susceptible d'atteindre les objectifs stratégiques sans entraîner de coûts de mise en conformité excessifs, et en réduisant considérablement la charge administrative.

Les règles renforcées en matière de protection des données devraient générer certains coûts de mise en conformité supplémentaires, notamment pour les responsables du traitement des données effectuant des traitements à risques. Mais un solide régime de protection des données peut aussi donner un avantage concurrentiel à l'économie de l'Union, car le niveau supérieur de protection et la diminution des incidents et violations qui devrait en résulter sont susceptibles de stimuler la confiance des consommateurs. Contraindre les entreprises européennes à adopter des normes élevées en matière de protection des données peut également leur être bénéfique à long terme : elles pourraient ainsi devenir des leaders mondiaux en matière de technologies améliorant la protection de la vie privée ou de solutions de protection des données dès la conception, attirant ainsi des entreprises, des créations d'emplois et des investissements dans l'Union européenne.

En outre, pour les entreprises qui exercent leurs activités sur le marché intérieur de l'Union, l'harmonisation renforcée rendra le traitement transfrontière des données à caractère personnel plus simple et moins onéreux. Ces entreprises devraient ainsi être tout particulièrement incitées à étendre leurs activités au-delà des frontières et à profiter des avantages du marché intérieur, ce qui aura des effets bénéfiques à la fois pour les consommateurs et pour l'économie européenne dans son ensemble.

L'option privilégiée apporte également une solution équilibrée au problème n° 3, puisqu'elle renforce les droits des personnes physiques, comble les lacunes et réduit les incohérences en ce qui concerne la protection des données dans le domaine de la coopération policière et judiciaire en matière pénale, tout en facilitant la coopération en matière de répression et en respectant les spécificités et les besoins opérationnels de ce secteur.

## 8. SUIVI ET EVALUATION

Le suivi et l'évaluation de l'impact de l'option privilégiée se concentreront sur des éléments tels que l'utilisation des nouveaux instruments introduits par la réforme, les pouvoirs et les ressources des autorités nationales chargées de la protection des données, les sanctions infligées pour les infractions à la législation en la matière, le temps et les moyens financiers consacrés par les responsables du traitement des données à la mise en conformité, et le développement de la confiance des personnes physiques à l'égard de la protection de leurs données à caractère personnel dans l'environnement en ligne.