Consultation publique sur le Règlement européen Sur la protection des données

SYNTHESE DES CONTRIBUTIONS

Le 16 juin 2016, la CNIL a lancé une consultation publique sur le règlement européen à destination des professionnels, afin de recueillir les questions concrètes, les difficultés d'interprétation et des exemples de bonnes pratiques suscités par le texte. Les contributions nourrissent les travaux du G29, qui adoptera des lignes directrices opérationnelles sur les différentes thématiques soumises à consultation.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

Les contributions reçues au sujet du délégué à la protection des données

La consultation relative au délégué à la protection des données a fait l'objet de 172 contributions directes sur le site et une dizaine de contributions de grandes fédérations professionnelles et cabinets de conseil particulièrement actifs aux cotés des CIL de tous horizons.

172 contributions
423 Votes

Les principales questions posées :

Les contributions se sont articulées autour de trois types de questions :

- 1. Comment interpréter opérationnellement les dispositions du RGPD ?
- 2. Que deviennent certains outils et pratiques issus de la LIL ?
- 3. Comment évoluera le rôle de l'autorité nationale dans sa relation avec les délégués ?

1. Dans quels cas dois-je désigner un délégué ?

https://www.cnil.fr/fr/consultation-reglement-europeen/dpo/dans-quels-cas-dois-je-designer-un-dpo

36 contributions – 95 votes

- Que signifie « *grande échelle* », « *activités de base* », « *suivi régulier et systématique* » ? cf. article 37.1
- Quelles sont les modalités de transformation des CIL en délégués : sera-ce automatique ou pas ?
- Quelle coexistence du CIL et du délégué après 2018 ?
- Quand pourra-t-on désigner un délégué auprès de la CNIL ? avant mai 2018 ?
- La CNIL validera-t-elle le caractère obligatoire ou non d'une désignation pour un organisme ?

2. Qui peut être un délégué ?

https://www.cnil.fr/fr/consultation-reglement-europeen/dpo/qui-peut-etre-dpo

46 contributions – 169 votes

- Faut-il définir un niveau de formation minimum ou une forme de « certification » OU *a contrario* ne pas définir de certification et laisser toute latitude aux entreprises pour choisir leurdélégué ?
- Quel profil professionnel est recommandé pour être délégué : juriste, technique, audit… ?
- Préciser ce qu'est un conflit d'intérêts – qui ne pourra pas être délégué ?

La CNIL validera-t-elle les désignations sur la base de critères déclaratifs, comme aujourd'hui ?

Les attentes formulées à l'égard des régulateurs peuvent être ainsi résumées :

- Prévoir un référentiel « délégué ou DPO » pour développer de bonnes pratiques de désignation
- ¨Proposer des ateliers sur le changement apporté pour les CIL>DPO, organiser des ateliers par secteur, renforcer l'information sur le RGPD en général

3. Dans quels cas et comment mutualiser ?

https://www.cnil.fr/fr/consultation-reglement-europeen/dpo/dans-quels-cas-et-comment-mutualiser

19 contributions – 17 votes

- Pour la mutualisation dans les organismes publics, que signifie mutualiser *« compte tenu de sa taille et de son organisation »* ?
- Pour la mutualisation dans les organismes privés, que signifie : *« facilement joignable à partir de chaque lieu d'établissement»* ?
- Plusieurs contributions se sont également montrées favorables à une certaine souplesse dans l'organisation et dans le périmètre de la désignation mutualisée (dans un même groupe, avoir des filiales mutualisées et d'autres pas, par exemple)

4. Quels moyens pour le délégué ?

https://www.cnil.fr/fr/consultation-reglement-europeen/dpo/quels-moyens-pour-le-dpo

16 contributions – 38 votes

Plusieurs propositions ont été formulées :

- Donner des indications pour évaluer le temps et les moyens à allouer à la fonction
- Etre formé aux techniques d'audit et contrôle interne en plus des connaissances des règlementations nationales et européennes
- Proposer des clauses types à inclure dans les contrats avec les sous-traitants
- Créer plus de guides prescriptifs de règles et bonnes pratiques pour être respecté en interne (sécurité, notification de violations)
- Préciser ce que signifie « *être associé d'une manière appropriée et en temps utile* » (donner des exemples)

5. Quelles missions pour le délégué ?

https://www.cnil.fr/fr/consultation-reglement-europeen/dpo/quelles-missions-pour-le-dpo

20 contributions – 34 votes

Plusieurs questions ou observations ont été formulées :

- Que devient la tenue du bilan du CIL ?
- Quel sera précisément le rôle du délégué dans l'initiative et dans la réalisation de l'analyse d'impact relative à la protection des données ?
- Quelles conséquences en interne en cas de non-respect des conseils du DPO ?

- Le délégué devrait pouvoir être en charge de la tenue du registre des activités de traitements
- Il faudrait préciser le rôle du délégué en matière de notification de violation de données (information ou pas)
- Il faudrait promouvoir les bonnes pratiques en la matière.

6. Autres sujets concernant le délégué

https://www.cnil.fr/fr/consultation-reglement-europeen/dpo/autres-sujets-concernant-le-dpo

35 contributions – 70 votes

- Le délégué peut-il voir sa responsabilité pénale engagée du fait qu'il *« contrôle le respect du RGPD »* ?
- Peut-on, et si oui comment, désigner plusieurs DPO dans une même structure (désignation partielle par catégories de traitement) ?
- Quid du règlement intérieur national des avocats qui prévoit les modalités d'exercice de la fonction de CIL pour un avocat ?
- Communicabilité du registre à toute personne ? Information préalable des IRP lors de la désignation ? Que deviennent toutes les dispositions du décret du 20 octobre 2005 – article 42 et ss.
- Quid du « *one-stop shop* » pour les multinationales qui n'ont pas de siège dans l'Union européenne (mais en Suisse, par exemple) mais de multiples filiales (de taille modeste) dans chaque pays de l'UE? Où placer le DPO ?
- Publication des coordonnées du délégué ou de l'identité complète ?

Verbatim

> *Quelques interrogations subsistent sur la responsabilité du DPO:*
>
> *Est-il responsable personnellement pénalement ? En cas de manquement du Responsable de traitement à ses obligations, le DPO peut-il être licencié pour faute ? Le DPO est-il responsable en cas de manquement de son responsable de traitement?*

> *Le DPO exercera-t-il une fonction unique ou pourra-t-il cumuler celle-ci avec une autre fonction?*

Le Fablab du 26 juillet (synthèse)

Le FabLab a confirmé les attentes de précisions et le besoin de partage de bonnes pratiques attendu dans les « Guidelines DPO ». Certaines discussions viennent compléter la consultation, telles que :

- Les dispositions du règlement s'appliquent-elles lorsque le délégué est désigné volontairement (hors cas de désignation obligatoire prévus par l'article 37.1) ?
- Le délégué pourrait-il être constitué d'une équipe ? Le délégué peut-il être une personne morale ?

- Proposer des clauses types à inclure dans le contrat avec le délégué externe
- Que signifie « *contrôler le respect* » du règlement (art. 39.1. b) ?
- Existe-t-il des spécificités pour les petites/moyennes entreprises ?

A retenir

On retiendra les fortes attentes de clarifications des CIL et organismes et fédérations professionnelles qui veulent se préparer dès maintenant et de façon pérenne à la mise en œuvre concrète de leurs futures obligations.

Plan d'action G29/CNIL

Dans le cadre du plan d'actions 2016 du G29, des lignes directrices seront publiées pour accompagner de façon pragmatique les responsables de traitements, les sous-traitants et les futurs DPO.

Pour assurer sereinement ce changement d'échelle, la CNIL réalisera également dans ce contexte des actions de communication auprès des organismes ayant actuellement un CIL et auprès des fédérations professionnelles concernées par la désignation obligatoire (courriers spécifiques, fiches pratiques). Les ateliers CIL seront enrichis (format, volume et contenus).

Les contributions reçues au sujet du droit à la portabilité

La consultation relative au droit à la portabilité a fait l'objet de 111 contributions. On constate une forte participation du secteur privé, exprimant de nombreuses interrogations sur le périmètre de ce nouveau droit, les charges induites par son exercice et les conséquences du droit à la portabilité en matière de concurrence.

111 contributions
154 votes

Les principales questions posées :

Il ressort de la consultation 3 types de contributions:

1. Quelles sont les nouvelles opportunités et contraintes liées au droit à la portabilité ?
2. Sur quelles données porte ce nouveau droit ?
3. De quelle manière répondre aux personnes exerçant ce nouveau droit ?

1. Le droit à la portabilité : quelles opportunités ?

https://www.cnil.fr/fr/consultation-reglement-europeen/portabilite/le-droit-la-portabilite-quelles-opportunites

21 contributions – 23 votes

De manière générale, le droit à la portabilité est perçu comme un outil permettant de renforcer la confiance des citoyens dans les traitements, en apportant une transparence et un contrôle accrus sur les données traitées. Si le bénéfice de ce droit est reconnu, des organismes s'inquiètent des contraintes et investissements additionnels qu'impliquera sa mise en œuvre.

- Les bénéfices attendus de la mise en œuvre de ce nouveau droit sont du point de vue du citoyen :
  - une reprise de contrôle sur ses données et la possibilité de changer aisément de prestataire, de manière à ne plus être « captif » d'un service ;
  - une meilleure visibilité quant à la nature des données collectées y compris passivement (données de localisation par exemple) ;
    l'opportunité de rééquilibrer leurs relations avec des fournisseurs de service « gratuits », sous réserve que la procédure permettant d'exercer ce droit ne soit pas trop complexe ; Le droit à la portabilité est aussi perçu comme un moyen concret de garantir le droit à l'autodétermination informationnelle au niveau européen ;
- Du point de vue des organismes (essentiellement privés), le droit à la portabilité est positivement perçu comme :
  - un moyen de redonner confiance au client dans l'exploitation que font les entreprises de ses données ;
  - un facteur de développement de la concurrence et du marché de l'Internet des objets (IoT);
  - un moyen de concourir à l'objectif de libre circulation des données en Europe ;
  - une incitation en interne à mieux maîtriser et assurer le suivi des données personnelles traitées, en tant que premier pas vers la mise en œuvre de la responsabilisation des entreprises (l' «accountability »).
- La création de ce nouveau droit génère toutefois des craintes chez les organismes notamment privés :

- quant au risque de renforcer le déséquilibre concurrentiel entre sociétés européennes directement soumises à l'obligation de répondre au droit à la portabilité et sociétés notamment américaines qui souhaiteraient contourner ces règles ;
- quant au coût immédiat de la mise en œuvre de ce droit (développement d'extractions automatisées de bases de données par exemple) qui ne pourra être facturé au client et sera répercuté dans les coûts de gestion, donc dans le prix payé par le client ;
- quant à leur niveau de responsabilité en cas de mésusage de la donnée ou de transmission de données non actualisées à la personne concernée.

2. Quelles limites au droit à la portabilité ?

https://www.cnil.fr/fr/consultation-reglement-europeen/portabilite/quelles-limites-au-droit-la-portabilite

34 contributions – 59 votes

Les contributions à cette partie ont essentiellement consisté en des questionnements qui seront pris en compte par la CNIL dans le cadre de ses réflexions sur l'étendue du droit à la portabilité.

- De manière générale, les organismes s'interrogent :
  - sur la « portabilité » :
    - des données relatives au foyer, relatives à l'activité bancaire, des contenus partagés sur une plateforme, des messages (mail, tweet, commentaire sur un billet de blog, etc) écrit par un tiers et envoyés à la personne concernée ;
    - des données fournies de manière passive, générées par l'activité de la personne concernée sur un site, lors de l'utilisation d'un service, etc.
    - des données collectées dans le cadre de la recherche scientifique ;
    - des données collectées au titre de « l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement », notamment par les collectivités locales et mairies ;
  - sur la manière d'assurer la protection des droits des tiers, lorsque des données les concernant sont incluses dans la portabilité ;
  - sur l'obligation de fournir des données à l'état brut ou sur la nécessité de les retravailler et de vérifier leur exactitude ainsi que l'absence de protection au titre du secret des affaires ou de la propriété intellectuelle, avant transmission à la personne concernée ou à un autre organisme ;
  - sur la possibilité d'arguer du coût de mise en œuvre de la portabilité pour en limiter l'étendue ;
  - sur la possibilité de refuser de répondre à une demande en cas de doute sur l'identité du demandeur ;
  - sur la manière de s'assurer de l'identité de la personne lorsque la demande est faite à distance.

3. Dans quels formats transférer les données ?

https://www.cnil.fr/fr/consultation-reglement-europeen/portabilite/dans-quel-format-transferer-les-donnees

16 contributions – 7 votes

En résumé, les contributions ont permis de dégager des pistes de solutions pratiques permettant de standardiser le format de transmission à moindre coût et de s'inspirer de dispositifs existants.

- De nombreux procédés actuels peuvent être réutilisés, par exemple l'EDI_ Echange de données informatisé, qui existe depuis longtemps dans le domaine industriel, les modélisations telle que HR-XML, le format FEP utilisé pour répondre à la DGFIP, etc. ;

- Il conviendrait de favoriser les formats libres/non propriétaires pour assurer une réutilisation à moindre frais, facilitant ainsi la concurrence, mais aussi l'auto-hébergement ;
- La prise en compte de la sémantique est centrale pour permettre une « compréhension mutuelle » des données ;
- Le développement d'interfaces de programmation applicative (APIs) documentées fondées sur un standard ouvert, sans clé de licence spécifique, pourrait être encouragé afin que chaque utilisateur puisse y recourir facilement avec les outils de son choix ;
- Il est toutefois important de laisser à chaque secteur une certaine liberté d'organisation quant aux modalités pratiques de mise en œuvre du droit à la portabilité ; une approche commune sectorielle pourrait ainsi être privilégiée sous forme de référentiel et standards ;
- La possibilité de fournir au titre du droit à la portabilité un condensé des informations et non les données brutes de manière exhaustive, doit être clarifiée.

4. La portabilité appliquée à votre secteur d'activité

https://www.cnil.fr/fr/consultation-reglement-europeen/portabilite/la-portabilite-appliquee-votre-secteur-dactivite

19 contributions – 32 votes

- Il est nécessaire d'organiser la portabilité par secteur d'activité, la transmission de données d'un acteur à un autre ayant *a priori* plus de sens au sein d'un même secteur (par exemple, le domaine de l'assurance, de la santé, de l'automobile) entre organismes proposant un service équivalent.
- Le droit à la portabilité ne pouvant concerner que les données traitées après consentement de la personne ou dans le cadre de l'exécution d'un contrat, les acteurs d'un même secteur pourraient utilement identifier les services potentiellement concernés par ce droit et identifier des solutions communes s'agissant de ces services.
- Chaque secteur souligne les spécificités en termes de nature de données traitées, de format de traitement et de transmission qui leur sont propres et qui peuvent en même temps différer entre acteur.
- Lorsque le traitement de la donnée implique la participation de plusieurs acteurs (au titre de l'hébergement, de l'analyse et de la mise à disposition), il conviendra de déterminer quel acteur sera chargé de répondre aux demandes de portabilité

5. Autres sujets en lien avec le droit à la portabilité

https://www.cnil.fr/fr/consultation-reglement-europeen/portabilite/autres-sujets-en-lien-avec-le-droit-la-portabilite

18 contributions – 33 votes

Cette section a permis de recenser les questions diverses se rapportant à la mise en œuvre du droit à la portabilité.

- La portabilité pourrait-elle être directement demandée par une entreprise concurrente sollicitée par la personne concernée ?
- De quelle manière assurer la sécurité de la transmission des données « portées » ?
- De quelle manière articuler le droit d'accès garanti par le règlement, le droit à la récupération et à la portabilité des données introduit par le PJL pour une République Numérique et le nouveau droit à la portabilité ?
- Quel est l'apport du droit à la portabilité par rapport à un droit d'accès permettant d'obtenir une réponse sous forme et par voie électronique ?

- Comment porter à la connaissance des personnes la procédure permettant d'exercer le droit à la portabilité ?

Verbatim

> *Le bénéfice indirect est de redonner confiance au client dans l'exploitation que font les entreprises de ses données. Et donc à moyen terme, de renforcer les services...mais cela prendra du temps à mon avis.*

> *En ce qui concerne les citoyens/consommateurs, ce nouveau droit, qui s'inscrit comme un prolongement du droit d'accès aux données, va dans le sens de la création d'un droit à l'autodétermination informationnelle au niveau européen.*

> *La portabilité des données peut être bénéfique pour les utilisateurs comme pour les entreprises. Elle peut, dans le domaine du Cloud computing, faciliter le déploiement d'applications complexes, maximiser les capacités d'adaptation des entreprises aux futures évolutions du marché, aux innovations, ou encore aux changements de l'environnement réglementaire.*

> *Mis en œuvre de façon pragmatique (prise en compte des contraintes techniques et limitation aux cas où il est strictement nécessaire à la protection des droits et libertés des personnes concernées), le droit à la portabilité pourra être vu comme un moyen pour les entreprises de mieux maitriser les données personnelles qu'elles traitent dans le cadre de la mise en œuvre de l' accountability .*

> *Quelques idées pour assurer que les formats/API soient réalisés de manière suffisamment pratique et "sincère". Format fondé sur un standard libre reconnu (xml, json, yaml, autre...). C'est indispensable mais pas suffisant pour assurer l'interopérabilité : en effet les données structurées peuvent être de nature complexe, liées à un outil particulier, donc difficiles à réimporter (cas typique des formats Word fondés sur XML).*

> *La mise à disposition des données étant très variable d'un secteur d'activité à un autre, il est recommandé de faire primer la liberté d'organisation des modalités pratiques de mise à disposition.*

Le Fablab du 26 juillet

Les participants se sont accordés sur l'intérêt de la portabilité pour faciliter le passage d'un service à un autre et rééquilibrer les relations entre fournisseurs de services et consommateurs.
Toutefois, l'étendue du droit à la portabilité doit être précisée, notamment en utilisant des exemples, pour apporter sécurité juridique aux organismes et visibilité aux personnes concernées. Des lignes directrices pratiques doivent être éditées, en tenant compte des difficultés pratiques des organismes.
Le droit à la portabilité ne doit notamment pas conduire à divulguer des informations couvertes par le secret des affaires ou créer des coûts importants qui, *in fine*, seront répercutés sur le consommateur.
La notion de donnée « fournie par la personne concernée » a été débattue, au regard de l'esprit initial du législateur qui visait les données chargées par la personne concernée sur un réseau social notamment.
Enfin, les participants ont souligné la nécessité de s'organiser par secteur d'activité dans un premier temps et d'utiliser des formats de transmission adaptables dans tous les secteurs, pour « casser les silos », dans un second temps.

A retenir

On retiendra de nombreuses incertitudes des organismes quant à l'esprit de ce nouveau droit et des inquiétudes quant au coût lié à sa mise en œuvre. Ils souhaitent anticiper dès à présent les procédures à mettre en place pour répondre à leurs nouvelles obligations et sont demandeurs de clarifications quant au périmètre réel du droit à la portabilité, en fonction duquel les actions à mettre en œuvre pourront être définies. De manière assez prévisible, les professionnels souhaitent limiter au strict minimum ce droit, là où les représentants de la société civile souhaitent l'étendre de manière à encourager les citoyens à reprendre en main leurs données et à en réinventer l'usage.

Plan d'action G29/CNIL –

Des lignes directrices sont actuellement en cours de rédaction au sein du sous-groupe technologie du G29. Cet avis a vocation à clarifier le périmètre du droit à la portabilité, en tenant compte des nombreux exemples fournis par les professionnels lors de la consultation notamment, et à préciser les modalités de réponse à adopter par les organismes. Il sera rendu public.

Les contributions reçues au sujet de la certification

La consultation relative à la certification a fait l'objet de 93 contributions en ligne auxquelles s'ajoutent celles de fédérations professionnelles.

93 contributions
129 Votes

Les principales questions posées :

Les contributions ont porté sur trois types de questions :

- 1. Comment évoluera le rôle de l'autorité nationale dans le cadre de la labellisation/certification ?
- 2. Quelle articulation des futurs labels avec les outils existants ?
- 3. Quel domaine et quelle portée aura la certification ?

1. Qui doit délivrer des certifications/des labels ?

https://www.cnil.fr/fr/consultation-reglement-europeen/certification/qui-doit-delivrer-des-certifications

34 contributions – 65 votes
Les contributions ont notamment porté sur les aspects suivants :

- Certification au niveau européen, ou à défaut une certification au niveau national avec reconnaissance mutuelle ;
- Coexistence difficile des certifications « CNIL » et des certifications délivrées par des organismes de certification ;
- Rédaction des référentiels à effectuer par les régulateurs en concertation avec les entreprises et futurs évaluateurs, en vue d'homogénéiser les pratiques des différents organismes de certification ;
- Approbation par la CNIL des référentiels privés, élaborés par des organismes de certification pour assurer une cohérence avec les labels des régulateurs, tout en accompagnant l'innovation des acteurs sectoriels.
- En cas de certification délivrée par des organismes privés, il y a un risque de report des coûts d'audit, de reporting, etc sur le coût des produits et services délivrés par les entreprises.

2. Que faut-il certifier/labelliser en priorité ?

https://www.cnil.fr/fr/consultation-reglement-europeen/certification/que-faut-il-certifier-en-priorite

11 contributions – 5 votes

- Les produits et services en lien avec les données de santé
- Les solutions de surveillance de bases de données

- Les services de l'Etat (au sens large, incluant les organismes en charge d'une mission de service public)
- Les techniques d'anonymisation
- Les moteurs de recherche
- Les réseaux sociaux

3. Quels sont les besoins spécifiques des micro, petites et moyennes entreprises ?

https://www.cnil.fr/fr/consultation-reglement-europeen/certification/quels-sont-les-besoins-specifiques-des-micro-petites-et-moyennes-entreprises

8 contributions – 4 votes

- Aide pour le montage des dossiers de certification
- Coût réduit
- Démarche simple

4. Quand faut-il retirer une certification/un label ?

https://www.cnil.fr/fr/consultation-reglement-europeen/certification/quand-faut-il-retirer-une-certification

8 contributions – 17 votes

- Instauration de lanceurs d'alertes pour signaler le non-respect de la certification
- Possibilité de dépôt d'avis positifs ou négatifs concernant le traitement des données à caractère personnel par les entreprises labellisées
- Retrait effectif après une procédure contradictoire avec mise en demeure de l'organisme à l'occasion de laquelle celui-ci peut proposer un plan correctif
- Publicité du dépôt

5. Autres sujets concernant la certification/les labels

https://www.cnil.fr/fr/consultation-reglement-europeen/certification/autres-sujets-concernant-la-certification

32 contributions – 38 votes

- Articulation avec les labels déjà délivrés
- Articulation entre les codes de conduite et la certification
- Certification d'établissements appartenant à un même réseau

Verbatim

> *Il n'apparaît pas contradictoire que la CNIL puisse approuver des référentiels privés, élaborés par les*

organismes de certification, afin d'assurer une parfaite cohérence avec les labels des régulateurs tout en accompagnant l'innovation des acteurs sectoriels.

> *Multiplier les organismes de certification n'est-il pas un danger ?*
>
> *Pour les PME en particulier, tout nouveau processus de certification ou labellisation devra être le plus simple et le moins coûteux possible.*

> *Le retrait de certification doit se faire au terme d'un processus contradictoire.*

> *Est-ce que, comme pour les codes de conduite, ces mécanismes de certifications et de labels peuvent être perçus comme un nouvel outil aux côtés des BCR, des clauses types, dans le cadre d'opérations de flux transfrontières ?*

Le Fablab du 26 juillet

A l'occasion du Fablab, les participants ont discuté tout particulièrement des points suivants :

- Quel modèle pour développer les mécanismes de certification (sceau, label, marque…) ? : Plusieurs schémas peuvent coexister, selon le secteur concerné. Toutefois, pour créer de la confiance, la certification européenne doit garantir un niveau élevé et homogène des normes utilisées.
- Les critères d'accréditation des organismes de certification : les autorités de protection des données devraient exiger de la part des organismes nationaux d'accréditation, l'insertion, dans leur référentiel général d'accréditation, de critères spécifiques « protection des données ». En effet, ces derniers constituent un gage de compétence en la matière de la part des organismes accrédités.
- Le schéma d'accréditation : mise en place mais également contrôles ; la certification doit porter essentiellement sur la protection des données et non sur la sécurité informatique (ce qui justifie qu'elle ne soit pas intégralement prévue par les normes ISO existantes).
- L'efficacité et l'utilité de la procédure de certification : nécessité de mettre en place des contrôles fiables.

A retenir

On retiendra les fortes attentes des CIL, organismes et fédérations professionnelles qui veulent se préparer dès maintenant et de façon sécurisée à la mise en œuvre concrète de leurs futures obligations. Ainsi, au-delà des incontournables actions de communication (courriers aux responsables de traitement et aux fédérations professionnelles, informations sur le site de la CNIL, interventions, ateliers CIL spécifiques), des supports et outils didactiques seront développés par les autorités de protection des données.

Les contributions reçues au sujet de l'analyse d'impact sur la protection des données (DPIA/PIA)

La consultation relative à l'analyse d'impact relatives à la protection des données (Data Protection Impact Assessment – DPIA – ou plus communément Privacy Impact Assessment – PIA) a fait l'objet de 98 commentaires.

98 contributions
215 votes

Les principales questions posées

Les contributions ont porté sur quatre types de questions :

1. Quand mener un DPIA ?
2. Comment réaliser un DPIA ?
3. Qui fait quoi dans un DPIA ?
4. Autres questions autour des DPIA

1. Quand mener un DPIA ?

https://www.cnil.fr/fr/consultation-reglement-europeen/eivp/quand-mener-une-eivp

41 contributions – 139 votes

Les contributions ont notamment porté sur les propositions suivantes :

- Démarche de la CNIL : préciser tout ce qui est flou, associer les acteurs économiques, fournir des critères et exemples, justifier, faire des tests, mettre à disposition et harmoniser au niveau européen ;
- Ce qui devrait être considéré pour établir les listes : impacts, besoins de sécurité, nature des données, nombre de personnes concernées, nombre de sous-traitants, l'étude juridique, mais aussi éviter trop de précision sur un sujet lié aux nouvelles technologies, voire ne pas généraliser à toutes les structures ;
- Ce qui devrait être inclus : les avis divergent (rien de plus que les exemples du 35.3 pour laisser l'organisme décider, ou uniquement le cas où aucune mesure n'est prise, ou systématiquement, puisque tous les traitements engendrent des risques !) ; plusieurs cas sont mis en évidence (RH, sites web, administrations, hôpitaux…) et des questions sont posées (le terme « grande échelle » concerne-t-il le big data ? le volume de données ou de personnes concernées ? les « nouvelles technologies » sont-elles toutes celles mises en œuvre pour la première fois par un organisme ? la publicité comportementale est-elle du «profilage ? la question n'est-elle pas redondante avec le fait de mener le DPIA ?) ;
- Ce qui devrait être exclu : tout ce qui n'est pas dans la liste des inclusions, normes simplifiées, traitements ayant déjà fait l'objet de formalités (sauf quand ils sont modifiés), données comptables ou de marketing direct, ou encore quand des mesures sont prévues ;

- Moment où mener le DPIA : quel délai précédant la mise en œuvre du traitement le DPIA ? faut-il considérer qu' « avant le traitement » ne s'applique pas aux phases préalables à la mise en œuvre complète (BUILD, POC) pour alimenter le DPIA de leurs résultats ?
- Calendrier et traitements existants : les traitements existants doivent-ils faire l'objet d'un DPIA ? la date d'application est-elle basée sur la date de création du traitement ?

2. Comment réaliser un DPIA ?

https://www.cnil.fr/fr/consultation-reglement-europeen/eivp/comment-realiser-une-eivp

27 contributions – 40 votes

Les propositions suivantes ont été formulées :

- sur la démarche méthodologique : les guides PIA sont jugés tantôt adaptés, tantôt complexes; une méthode simple serait appréciée ; des références à d'autres outils (EBIOS, ISO 29134…) sont faites ; il est demandé de tester la démarche avec des responsables de traitements (RT) et d'harmoniser au niveau européen, et si des associations professionnelles peuvent créer leur propre démarche
- sur l'outillage complémentaire : outil en ligne sur la base des guides PIA, outil rapide (tableur, formulaire, 2 trames selon des critères contextuels ou selon le DPO : une légère/systématique et l'autre basée sur les guides PIA), adaptations sectorielles ou par sensibilité ; seront-ils obligatoires ?
- sur la démarche détaillée : une unique réunion avec les parties prenantes, garder l'avis des personnes concernées optionnel et non contraignant ; les questions concernent l'impact des codes de conduite sur la réduction des risques, les preuves relatives au DPIA et l'avis des personnes concernées (quand et comment est-il demandé ? que faire si l'avis est négatif ?…)
- sur les suites du DPIA (article 35.11) : dans quels cas faut-il évaluer si le traitement est effectué conformément au DPIA ? est-ce une révision du DPIA ou le moyen de constater la modification du risque ? à quelle fréquence le DPIA doit-il être mené ? révision annuelle ?

3. Qui fait quoi dans un DPIA ?

https://www.cnil.fr/fr/consultation-reglement-europeen/eivp/qui-fait-quoi-dans-une-eivp

14 contributions – 11 votes

- d'une manière générale : les rôles peuvent être ceux décrits dans les guides PIA, ou bien adaptés, ou laissés totalement à l'appréciation de l'organisme ; la validation relève de l'organisme ;
- le RT : il assume la responsabilité mais « ce n'est pas son job », et il peut imposer de mener un DPIA sur tous les traitements ;
- le sous-traitant : il est demandé de préciser comment il doit assister le RT et suggéré que cela relève de l'organisation interne de chaque entreprise ;
- le DPO : il propose de mener un DPIA, accompagne le RT (ex : chef de projet DPIA), juge de la pertinence de l'appréciation des risques, juge si le risque résiduel est acceptable, et peut utilement se constituer une base de connaissances sur son contexte ; il est notamment demandé si des lignes directrices sur son implication seront publiées par la CNIL ;
- le responsable de la sécurité des systèmes d'information (RSSI) : il accompagne le RT et pourrait proposer de mener un DPIA selon les besoins de sécurité des traitements ;

- le service en charge de l'informatique ou le RSSI : il mène l'étude de sécurité, qui est complétée par le DPIA ;
- les métiers : ils peuvent proposer de mener un DPIA, et interviennent dans l'acceptation des risques ;
- les personnes concernées : les questions concernent les conditions de la demande d'avis (dans quels cas ? quelle forme ? quand ? qui sont leurs représentants ?...)

4. Autres questions autour des DPIA

https://www.cnil.fr/fr/consultation-reglement-europeen/eivp/autres-questions-autour-des-eivp

16 contributions – 25 votes

- sur des points généraux relatifs aux DPIA : le DPIA est jugé comme un excellent outil pour vérifier et prouver la conformité ; les interrogations portent sur la réalisation conjointe de DPIA, la base juridique du 35.10 et la prise en compte des normes simplifiées ; il est également suggéré de partager les DPIA ;
- sur la consultation préalable de l'autorité (article 36) : les conditions doivent être précisées ; ne devrait-elle pas être systématique pour avoir un avis de la CNIL ? qui le déterminera ? que faut-il envoyer ? quel est l'objet (conseil, autorisation...) ? est-il public ? anonyme ? l'avis doit-il être respecté ? sera-t-il contrôlé ? il est proposé de mieux définir les délais du 36.2 et de partager les avis au niveau européen afin de guider les RT ;
- sur la formation : la CNIL fera-t-elle des ateliers ? il les faudrait opérationnels, avec des études de cas ; faire un kit d'accompagnement du DPO.

Verbatim

> *Il serait souhaitable que des critères soient publiés par la CNIL.*

> *Le guide PIA de la CNIL ne permet-il pas déjà de faire cela ?*

> *Il ne s'agit pas de refaire l'analyse de sécurité déjà faite par le RSSI mais de la compléter.*

> *Le G29 peut-il proposer une méthode d'analyse harmonisée pour mener une EIVP ?*

> *La CNIL envisage-t-elle de mettre en place des outils complémentaires pour aider le CIL/DPO à réaliser des PIA ?*

> *Quel sera exactement le rôle du DPO dans la décision de mettre en œuvre une analyse d'impact et dans le déroulement de cette dernière ?*

> *Article 36(1) : « Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque ». Ce critère est très subjectif et n'est pas clair.*

Le Fablab du 26 juillet

- Le DPIA est un outil de conformité dynamique, qui contribue à maintenir la sécurité, réduire les risques, déterminer les mesures pertinentes, prévenir les manquements légaux et mieux mettre en œuvre le *privacy by design* et *privacy by default*. C'est un outil nouveau et important, reconnu comme tel par le législateur dans la mesure où ne pas l'utiliser quand il est requis peut engendrer d'importantes sanctions.
- Le DPIA doit être mené par le responsable de traitement avant la mise en œuvre du traitement. La consultation préalable doit également avoir lieu avant la mise en œuvre du traitement. Les autorités de protection des données ne doivent être consultées que dans les cas de risques élevés. La documentation, d'un niveau de détail approprié, doit être tenue à disposition des autorités.
- Une liste des traitements requérant un DPIA doit être établie (article 35.3).
- Les considérants donnent des exemples qui peuvent aider à l'estimation de la gravité et de la vraisemblance des risques (ex : le considérant 75 sur les d'impacts sur les personnes concernées).
- Les autorités de protection des données devraient préciser les critères de l'article 35.3, définir une liste de traitements requérant un DPIA, harmonisée au niveau européen, et considérant les traitements existants ayant déjà fait l'objet d'une conformité à la loi nationale, guider sans être trop de prescription, en faisant en sorte que le DPIA soit approfondi mais pas complexe, contextualisé aux PME et évolutif, et clarifier comment gérer un DPIA avec une dimension pan-européenne (ex : envoyé à et évalué par uniquement l'autorité compétente).
- Ont également été soulignés le fait que les sociétés ont déjà mis en œuvre des processus proches du DPIA pour gérer les risques, les implications pratiques des traitements transfrontières, l'articulation d'un DIA avec les autres exigences de protection des données, et les modalités pour obtenir l'avis des personnes concernées ou de leurs représentants.

À retenir

En synthèse, les contributions font émerger un grand besoin de clarification, mais aussi des idées intéressantes qu'il conviendra de prendre en considération. Les points durs concernent les critères qui guideront la décision de mener un DPIA, l'harmonisation de la démarche au niveau européen, et la consultation préalable.

Plan d'action G29/CNIL

L'avis du G29 sur les DPIA et risques élevés, qui a pour but de proposer des interprétations aux exigences floues, devra ainsi tenir compte de ces commentaires.

L’outillage de la CNIL va également pouvoir être développé ou amélioré : logiciel, études de cas, révision des guides PIA.