FORMULAIRE DE DEMANDE

DE DELIVRANCE D’UN LABEL

*Délibération n°2017-219 du 13 juillet 2017 portant modification du référentiel pour la délivrance de labels en matière de procédures de gouvernance tendant à assurer la protection des données*

POUR UNE procédure de gouvernance tendant a assurer la protection des donnees

*Version du formulaire : Septembre 2017*

# Modalités de candidature

1. Le demandeur, candidat au label, peut être un organisme privé ou public disposant obligatoirement d’un délégué à la protection des données (DPO), personne physique ou personne morale, interne ou externe à l’organisme demandeur, mutualisé avec d’autres ou non.
2. Le présent formulaire doit être dûment rempli pour demander la délivrance d’un label à une procédure de gouvernance tendant à assurer la poreciton des données. Il permet d’expliquer comment chaque exigence du référentiel d’évaluation est satisfaite et de présenter ou de référencer les éléments permettant de le justifier.
3. Il est ainsi possible de compléter le formulaire par des éléments de justification, en respectant les conditions suivantes :
* tout document joint en tant que justification doit respecter la convention de nommage suivante (personnaliser les libellés entre crochets et retirer les crochets) :
LabelsCNIL-gouvernance-[nom du demandeur]-[libellé court désignant le document]-[année]-[mois]-[jour].[suffixe]
* tout document électronique doit être lisible par les logiciels de bureautique ou multimédia courants (.doc, .pdf, .txt, .rtf, .jpg…).
1. Le formulaire dûment rempli doit être envoyé à la CNIL avec l’ensemble des éléments de justification en pièces jointes :
* soit par le biais du formulaire de dépôt en ligne
* soit par courrier postal à l'adresse suivante :

**Commission Nationale de l'Informatique et des Libertés**

**3 Place de Fontenoy**

**TSA 80715**

**75334 Paris cedex 07**

Les informations recueillies font l’objet d’un traitement informatique destiné à permettre à la CNIL l’instruction des demandes de label qu’elle reçoit. Elles sont destinées aux membres et services de la CNIL. Vous pouvez exercer votre droit d’accès et de rectification aux informations qui vous concernent en vous adressant à

# Informations administratives[[1]](#footnote-1)

Les informations suivantes sont nécessaires pour échanger avec la CNIL dans le cadre de l’évaluation de la procédure de gouvernance tendant à assurer la protection des données, notamment en cas de compléments d’informations nécessaires à l’instruction de la demande.

## Organisme demandeur

|  |  |
| --- | --- |
| N° SIREN[[2]](#footnote-2) + NIC[[3]](#footnote-3) |       |
| Code NAF[[4]](#footnote-4) |       |
| \*Nom de l’organisme |       |
| Sigle (le cas échéant) |       |
| \*Adresse |       |
| \*Code postal |       |
| \*Localité |       |

## Contact[[5]](#footnote-5)

|  |  |
| --- | --- |
| Civilité |       |
| \*Nom |       |
| \*Prénom |       |
| Service |       |
| \*Adresse |       |
| \*Code postal |       |
| \*Localité |       |
| Téléphone |       |
| Télécopie |       |
| \*Adresse électronique |       |

# Informations relatives à la procédure de gouvernance tendant à assurer la protection des données[[6]](#footnote-6)

Les informations suivantes sont nécessaires pour identifier la procédure qui fait l’objet de la demande de délivrance de label et délimiter son périmètre.

|  |  |
| --- | --- |
| Présentation de la procédure de gouvernance des données personnelles au sein de l’organisme demandeur |       |

# Satisfaction des exigences du référentiel

L’évaluation de la procédure de gouvernance des données personnelles au sein de l’organisme demandeur sera faite au regard des tableaux suivants. Elle pourra être complétée via des échanges entre les évaluateurs et le demandeur.

## Evaluation du dispositif interne lié à la protection des données [[7]](#footnote-7)

| **Exigences** | **Moyens mis en œuvre (500 caractères maximum)** | **Eléments de justification [[8]](#footnote-8)(exemples ci-après ; modifier cette colonne selon les éléments envoyés)** |
| --- | --- | --- |
| **Exigences relatives à la politique de protection des données** |
| EOR01. Le demandeur met en place en interne une politique appropriée en matière de protection des données. Cette politique comprend l’ensemble des principes nécessaires pour garantir la mise en œuvre de traitements équitables et transparents, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées. Cette politique indique les coordonnées du demandeur, celles du délégué à la protection des données[[9]](#footnote-9), ainsi que les engagements du demandeur concernant le respect des principes énoncés par le règlement européen général sur la protection des données[[10]](#footnote-10), au regard notamment* de la mise en œuvre de traitements licites,
* du respect des droits des personnes,
* des éventuels transferts vers un pays tiers,
* des destinataires des données collectées,
* de la durée de conservation des données collectées,

des mesures de sécurité des données. |  | Politique de protection des donnéesCode de conduite approuvé |
| EOR02. Le demandeur porte à la connaissance des personnes extérieures concernées par ses traitements sa une politique en matière de protection des données et ce dans un format concis, transparent, compréhensible et aisément accessible.Cette politique comprend toute information nécessaire pour garantir la mise en œuvre de traitements équitables et transparents, compte tenu des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées. Cette politique indique les coordonnées du demandeur, celles du délégué à la protection des données, ainsi que les engagements du demandeur concernant le respect des principes énoncés par le règlement européen général sur la protection des données, au regard notamment :* de la mise en œuvre de traitements licites,
* du respect des droits des personnes,
* des éventuels transferts vers un pays tiers,
* des destinataires des données collectées,
* de la durée de conservation des données collectées,
* des mesures de sécurité des données.

Elle indique les mentions et engagements du demandeur énoncés dans le cadre de l’EOR01. |  | Politique de protection des donnéesCode de conduite |
| EOR03. Le demandeur garantit que le délégué à la protection des données contrôle le respect des politiques mises en place en matière de protection des données. Ces politiques sont réexaminées et actualisées si nécessaire, *a minima* tous les trois ans |  | Procédure de validationAudit |
| **Exigences relatives au délégué à la protection des données** |
| EOR04. Le demandeur a désigné un délégué pour l’ensemble des traitements mis en œuvre par l’organisme. |  | Tout document prouvant la désignation auprès de la CNIL ou d’une autre autorité nationale de contrôle |
| EOR05. Le demandeur prévoit que le délégué fait rapport directement au niveau le plus élevé de la direction de l’organisme. |  | Un organigramme de la structureUn exemple/modèle de bilan annuel d’activité et l’indication de la présentation annuelle |
| EOR06. Le demandeur précise clairement l’étendue des missions du délégué dans une lettre de mission ou dans un contrat. |  | Un document formalisant les missions du délégué |
| EOR07. Le demandeur s’assure que le délégué désigné dispose au moment de sa désignation des qualités professionnelles, connaissances juridiques spécialisées et pratiques en matière de protection des données requises. |  | CVTout document justifiant de l’expérience professionnelle du déléguéAbonnements juridiquesFormations juridiques et expériences en I&L |
| EOR08. Le demandeur justifie comment permettre au délégué d’entretenir ses connaissances spécialisées. |  | Suivi de formations, conférences, tables rondes, etc.Abonnements à des lettres d’information spécialisées |
| EOR09. Le demandeur justifie les ressources nécessaires et les conditions de travail fournies au délégué pour qu’il exerce ses missions.  |  | Tous éléments montrant, notamment : * le soutien de l’encadrement supérieur,
* le temps dont dispose le délégué pour exercer sa mission,
* le personnel,
* les moyens financiers,
* la formation continue,
* l’accès aux données,

l’absence de conflit d’intérêts |
| EOR10. Le demandeur s’assure que le délégué pilote la mise en conformité des traitements, dès leur conception et par défaut, et qu’il est associé systématiquement et en amont des réflexions sur toutes les questions relatives à la protection des données. |  | Procédure de validation des traitements |
| EOR11. Le responsable de traitement et, si nécessaire, le représentant du responsable de traitement tiennent, ou peuvent faire tenir par le délégué à la protection des données, un registre des activités de traitement, comprenant, *a minima* par traitement :* nom et coordonnées du responsable de traitement et le cas échéant du responsable conjoint du traitement, du représentant du responsable de traitement et du délégué ;
* la ou les finalités du traitement ;
* une description des catégories de personnes concernées ;
* une description des catégories de données à caractère personnel ;
* la durée de conservation associée à chaque catégorie de données ;
* les catégories de destinataires, y compris les destinataires dans des pays tiers ou des organisations internationales ;
* les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale (y compris leur identification) ainsi que les documents attestant de l’existence de garanties appropriées, conformément à l’article 49 paragraphe 1, 2ème alinéa du RGPD ;
* une description des mesures de sécurité techniques et organisationnelles (cf. article 32, paragraphe 1) ;
* l’existence ou non d’une sous-traitance (avec contrat de sous-traitance ou autre acte juridique définissant l’objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et droits du responsable de traitement).

 *OU, si la demande est formulée par le sous-traitant* :* nom et coordonnées du (ou des) sous-traitant(s) et de chaque responsable de traitement pour lequel le sous-traitant agit, ainsi que, le cas échéant, les noms et coordonnées du représentant du responsable de traitement ou du sous-traitant et du délégué ;
* les catégories de traitements effectués pour le compte de chaque responsable du traitement ;
* les transferts de données à caractère personnel vers un pays tiers ou une organisation internationale (y compris leur identification) ainsi que les documents attestant de l’existence de garanties appropriées, conformément à l’article 49 paragraphe 1, 2ème alinéa du RGPD;
* une description des mesures de sécurité techniques et organisationnelles.
 |  | Modèle de registre Clauses types Informatique et Libertés, utilisées par le demandeur, et conformes à l’article 28 RGPD |
| EOR12. Le demandeur justifie comment le délégué l’informe et le conseille, ainsi que les employés procédant au traitement, en matière de protection des données à caractère personnel. |  | Exemple d’action de sensibilisation menée par le délégué à la protection des donnéesModèle de support d’information, d’outils pédagogiquesPlanning des réunions annuelles entre responsable de traitement et DPD |
| EOR13. Le demandeur s’assure que le délégué est le point de contact avec l’autorité de contrôle, et qu’il coopère avec cette dernière. |  | Documents prouvant les échanges avec l’autorité de contrôle. |

## 3.1 Evaluation de la méthode de vérification de la conformité des traitements à la loi Informatique et Libertés et au règlement européen à la protection des données.

| **Exigences** | **Moyens mis en œuvre (500 caractères maximum)** | **Eléments de justification [[11]](#footnote-11)(exemples ci-après ; modifier cette colonne selon les éléments envoyés)** |
| --- | --- | --- |
| **Exigences relatives à l’analyse de la conformité** |
| EM01. Le délégué analyse les projets de traitements et les traitements en termes :* de finalité du traitement,
* de proportionnalité du traitement au regard de la finalité,
* de minimisation des données collectées au regard de la finalité,
* de licéité du traitement,
* de sécurité des données collectées,
* de durée de conservation des données collectées,
* de destinataires des données collectées,
* d’encadrement des relations avec les sous-traitants,
* d’information claire et préalable des personnes concernées,
* de conditions d’’exercice des droits des personnes,
* et le cas échéant d’encadrement des transferts de données hors Union européenne.

Le demandeur veille à documenter la manière dont ces principes sont respectés pour chaque traitement.  |  | Modèle type d’analyse des traitementsCode de conduite |
| EM02. L’analyse effectuée permet d’identifier les traitements susceptibles d’engendrer un risque élevé pour les droits et libertés des personnes concernées, pour lesquels il est nécessaire de réaliser une analyse d’impact relative à la protection des données. L’analyse d’impact relative à la protection des données comprend *a minima* :* une description systématique des opérations de traitement envisagées et des finalités, y compris l’intérêt légitime poursuivi,
* une évaluation de la nécessité et de la proportionnalité des opérations de traitements au regard des finalités,
* une évaluation des risques pour les droits et libertés des personnes concernées,
* les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du RGPD, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

La procédure du demandeur prévoit la possibilité de demander l’avis des personnes concernées. |  | Modèle d’analyse d’impact |
| EM03. L’analyse effectuée par le demandeur permet de déterminer les mesures techniques et organisationnelles adaptées au risque présenté par le traitement pour les personnes concernées. |  | Procédure interne de décision d’analyse d’impact. |
| EM04. La procédure du demandeur encadre le recours à des sous-traitants dans la mise en œuvre des traitements. A ce titre, elle impose le recours à un contrat définissant l’objet, la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et droits du demandeur. Le contrat respecte les prescriptions de l’article 28 du RGPD.La procédure du demandeur permet d’assurer que le sous-traitant auquel il recourt :* présente des garanties suffisantes concernant la mise en œuvre de mesures techniques et organisationnelles adaptées afin que le traitement réponde aux exigences du RGPD et garantisse la protection des droits des personnes,
* recourt lui-même à un sous-traitant uniquement avec autorisation préalable du responsable de traitement.
 |  | Contrat type avec ST ou exemples de contratsCode de conduite ou certification appliqués par un sous-traitant pour justification de ses garanties suffisantes. |
| EM05. La procédure du demandeur prévoit la réalisation d’une analyse permettant de déterminer les mesures techniques et organisationnelles adaptées au risque présenté par le traitement pour les personnes concernées.  |  | Exemple d’analyse |
| EM06. La procédure du demandeur prévoit que le délégué est consulté pour toute analyse d’impact et qu’il vérifie son exécution.Le délégué peut dispenser des conseils au responsable du traitement. Si ce dernier ne suit pas les observations formulées, la documentation de l’analyse d’impact relative à la protection des données doit en mentionner la raison. |  | Procédure interne et exemple de remontée d’observations au responsable de traitement. |
| **Exigences relatives à l’analyse de la conformité dans le temps** |
| EM07. La procédure du demandeur prévoit que les mesures techniques, organisationnelles et de mise en conformité, visées aux exigences EM01 et EM03, sont régulièrement testées, analysées et évaluées, afin de vérifier leur efficacité.  |  | Modèles de tests, analyses et évaluations des mesures techniques et organisationnelles, avec indication de périodicité. |
| EM08. La procédure du demandeur (responsable de traitement) prévoit un examen régulier de la conformité du traitement au regard de l’analyse d’impact visée à l’exigence EM01, et *a minima* lorsqu’il y a modification du risque présenté par l’opération de traitement.  |  | Exemple / modèle d’examen de la conformité du traitement au regard de l’analyse d’impact |
| EM09. La procédure du demandeur prévoit que les mesures correctives adoptées en cas de manquement constaté lors de l’examen de conformité sont documentées et régulièrement mises à jour. |  | Preuve de la documentation et de la mise à jour des mesures correctives. |

## Evaluation de la gestion des réclamations et incidents [[12]](#footnote-12)

| **Exigences** | **Moyens mis en œuvre (500 caractères maximum)** | **Eléments de justification [[13]](#footnote-13)(exemples ci-après ; modifier cette colonne selon les éléments envoyés)** |
| --- | --- | --- |
| **Exigences à la gestion des réclamations et à l’exercice des droits des personnes** |
| EG01. Le demandeur met en place une procédure facilitant l’exercice des droits des personnes (droit d’accès, de rectification, d’effacement, de limitation du traitement, à la portabilité, de définir le sort de ses données après son décès), comprenant, conformément à l’article 12 du RGPD et *a minima*les modalités : * d’identification/authentification de la personne concernée exerçant ses droits,
* permettant de respecter les délais de réponse.
 |  | Procédure d’exercice des droits des personnes |
| EG02. La procédure du demandeur prévoit que le délégué, en tant que point de contact des personnes concernées, pilote la gestion des demandes des personnes concernées relatives au traitement de leurs données et à l’exercice de leurs droits.  |  | Circuit (procédure) interne  |

|  |
| --- |
| **Exigences à la gestion des violations de données** |
| EG03. Le demandeur (responsable de traitement) met en place une procédure de notification d’une violation de données à caractère personnel à l’autorité de contrôle compétente, si possible dans les 72 heures après en avoir pris connaissance. Si le demandeur est sous-traitant, celui-ci doit notifier au responsable de traitement dans les meilleurs délais après en avoir pris connaissance.La notification à l’autorité compétente doit comporter *a minima*: * la nature de la violation,
* les catégories et nombre de personnes concernées par la violation,
* les catégories et nombre approximatif d’enregistrements de données à caractère personnel concernés,
* le nom et les coordonnées du délégué,
* les conséquences probables de la violation de données,
* ainsi que les mesures prises et/ou à prendre pour remédier ou atténuer les éventuelles conséquences négatives.
 |  | Procédure de notification d’une violation de données |
| EG04. Le demandeur met en place une procédure permettant, en cas de violation de données à caractère personnel susceptible d’engendrer un risque élevé pour les droits et libertés d’une personne physique, d’en informer les personnes concernées dans les meilleurs délais. Cette information doit comporter *a minima* :* la nature de la violation,
* le nom et les coordonnées du délégué,
* les conséquences probables de la violation de données,
* ainsi que les mesures prises ou qui vont l’être pour remédier ou atténuer les éventuelles conséquences négatives.
 |  | Procédure de notification d’une violation de données |

1. Les champs précédés d'un astérisque sont obligatoires. [↑](#footnote-ref-1)
2. Système d’Identification du Répertoire des Entreprises. [↑](#footnote-ref-2)
3. Numéro Interne de Classement. [↑](#footnote-ref-3)
4. Nomenclature des Activités Françaises. [↑](#footnote-ref-4)
5. À même de communiquer à la CNIL les compléments d’information nécessaires à l’instruction de la demande. [↑](#footnote-ref-5)
6. Tous les champs sont obligatoires. [↑](#footnote-ref-6)
7. Tous les champs sont obligatoires. [↑](#footnote-ref-7)
8. Modifier cette colonne selon les éléments de justification envoyés [↑](#footnote-ref-8)
9. Ci-après « le délégué »

 [↑](#footnote-ref-9)
10. Ci-après « RGPD » [↑](#footnote-ref-10)
11. Modifier cette colonne selon les éléments de justification envoyés [↑](#footnote-ref-11)
12. Tous les champs sont obligatoires. [↑](#footnote-ref-12)
13. Modifier cette colonne selon les éléments de justification envoyés [↑](#footnote-ref-13)