ANNEXE - 1

5.1 Registre des activités de traitement

Tenir un registre des traitements est une obligation légale. Le registre doit être tenu à jour par chaque service, dans son périmètre, au moyen de l'application informatique dédiée mise en place par le DPO. Le DPO centralise le registre global du gouvernement. Une mise à jour du registre est opérée à minima une fois par an, avant le 31 décembre.

5.2 Procédures

Le DPO établit les procédures transversales aux services (annexées à la présente circulaire). Elles doivent être portées à la connaissance de tout personnel. Tout personnel doit les appliquer. Les procédures transversales sont les suivantes :

- gestion des demandes d'exercice de droits,
- gestion des violations de données à caractère personnel,
- gestion des analyses d'impact relatives à la protection des données (AIPD).

En complément, chaque service met en place les procédures nécessaires à la gestion des obligations de la réglementation informatique et libertés, en s'aidant des modèles fournis dans la Boite à Outils pour la protection des données mise à disposition par le DPO. Par exemple, chaque service peut mettre en place une procédure de gestion des durées de conservation, gestion de la protection des données dès la conception, etc.

Ces procédures font l'objet de note(s) de service dument portée(s) à la connaissance des personnels (leur existence doit être incluse dans la note de service « sur les modalités d'application de la réglementation relative à la protection des données à caractère personnel au sein du service »).

5.3 Information et droits des personnes

Le service fixe, pour chaque traitement, les modalités d'information des personnes, l'adresse de contact et les personnes désignées pour traiter les demandes.

La gestion des demandes fait l'objet de la procédure prévue à l'annexe 2 ci-après.

Un registre répertorie les demandes d'exercice de droits et les suites qui y ont été réservées (dans l'application informatique dédiée mise en place par le DPO).

Le chef de service veille au strict respect des délais de réponse fixés par la réglementation, car ils exposent la collectivité à des sanctions.

5.4 Gestion des violations de données

Le signalement et la gestion des incidents de sécurité ayant pour effet de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles font l'objet de la procédure prévue à l'annexe 3 ci-après.

L'incident et le risque qu'il représente sont évalués dans ce cadre. Les violations de données entraînant un risque pour les droits et libertés des personnes font l'objet d'une notification à la CNIL, dans les 72 heures et, en cas de risque élevé, à la personne concernée dans les meilleurs délais. Ces notifications sont réalisées par le chef du service concerné après avis et avec le concours du DPO.

Un registre répertorie les violations de données et les suites qui y ont été réservées (dans l'application informatique dédiée mise en place par le DPO).

5.5 Sous-traitance

Chaque service doit s'assurer, lorsqu'il confie à un tiers (par exemple, un prestataire) le traitement de données à caractère personnel pour son compte, que ce tiers présente des garanties suffisantes quant au respect de la réglementation informatique et libertés.

Il doit en outre obligatoirement inclure dans le contrat des clauses dites de « sous-traitance de données à caractère personnel » conformes aux exigences de la réglementation informatique et libertés, en s'aidant des modèles fournis dans la Boite à Outils pour la protection des données mise à disposition par le DPO.

5.6 Sécurité des traitements

Les mesures de sécurité, tant techniques qu'organisationnelles, doivent être mises en œuvre afin de garantir un niveau de protection adapté au risque. Elles ont pour objet d'assurer l'intégrité, la disponibilité et la confidentialité des données traitées.

Ces mesures sont définies et mises en œuvre

- pour les traitements non informatisés par chaque chef de service, pour les traitements mis en œuvre dans sa structure ;
- pour les traitements informatisés, par la DSI s'agissant des mesures à caractère transversal déployées dans le périmètre d'intervention de la DSI, et par chaque chef de service pour les autres mesures.

Les mesures de sécurité sont documentées dans le registre des traitements et dans l'analyse d'impact lorsque celle-ci est requise.

5.7 Protection des données dès la conception

Tout nouveau projet de traitement de données doit s'inscrire dans une démarche organisée de protection des données dès la conception. Les chargés de projet peuvent s'aider du Kit RGPD du chargé de projet informatique et sollicitent leur RIL et le DPO.

5.8 Analyses d'impact

Une analyse d'impact est obligatoire pour les traitements qui présentent un risque élevé pour les droits et libertés des personnes, répondant aux critères fixés par le RGPD, la loi informatique et libertés, les lignes directrices du comité européen des données et les délibérations de la CNIL.

La réalisation de ces analyses est de la responsabilité des services, pour les traitements qui les concernent.

La réalisation d'une analyse d'impact fait l'objet de la procédure prévue à l'annexe 4 ci-après.

5.9 Sensibilisation et formation

Les services veillent à mettre en place des sessions de sensibilisation et une formation adaptée de leurs personnels à la protection des données et à la sécurité, via l'offre de formation de la Direction des talents et de l'innovation (DTI), au moyen de sessions adaptées à leurs métiers, au moyen des

MOOC mis en ligne par la CNIL et l'ANSSI. Ils doivent pouvoir justifier du nombre ou du pourcentage de leurs personnels ayant bénéficié de sensibilisations ou formations.

5.10 Transferts de données hors de l'union européenne

L'absence de transfert de données hors de la Polynésie française ou hors de l'Union européenne est à privilégier.

À défaut, lorsque des données à caractère personnel sont susceptibles d'être transférées vers un pays tiers à l'Union européenne, le service s'assure que ce Pays tiers bénéficie d'une décision d'adéquation de la Commission européenne ou que ce transfert s'appuie sur l'une des autres garanties prévues par la réglementation informatique et libertés. Il documente ces garanties dans le registre des traitements.

5.11 Traitements soumis à des formalités préalables auprès de la CNIL

Les traitements de données de santé ayant pour finalité la recherche, les études et les évaluations dans le domaine de la santé font encore l'objet de ces formalités. Lorsqu'elles sont requises, elles sont accomplies par le service concerné, après avis et avec l'appui du DPO.