POLITIQUE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Depuis la loi Informatiques et Libertés de 1978, des règles de gouvernance interne ont été mise en place dédiées à la protection des données ; celles-ci sont renforcées par l'application du règlement général sur la protection des données (RGPD).

1

ORGANISATION INTERNE ET IMPLICATION DE L'ENSEMBLE DES COLLABORATEURS

Autour d'une équipe dédiée à la protection des données personnelles : une protection efficace et décentralisée

Le CEA a désigné, en interne et auprès de l'Autorité de contrôle - la Cnil, un **Délégué à la protection des données** (DPD). Au sein de chaque direction, le DPD s'appuie sur un réseau de correspondants à la protection des données (CPD) et un réseau d'agents de sécurité des systèmes d'information (ASSI). Le DPD veille avec l'équipe des CPD aux respect des obligations du CEA en matière de protection des données : élaboration des procédures internes au CEA, information, mise à jour des registres. Chaque collaborateur est impliqué dans la protection des données personnelles : il est formé puis régulièrement informé sur le droit de la protection des données et sur les outils de gouvernance mis en œuvre au sein du CEA. Ces **informations et outils régulièrement mis à jour** sont accessibles sur l'intranet du CEA.

2

TRACABILITE ET CONTROLE DE LA LICEITE DES TRAITEMENTS

Pour une meilleure traçabilité et une revue régulière

Le CEA a également mis en place des procédures permettant de porter à la connaissance du DPD tout nouveau traitement ou toute modification d'un traitement de données à caractère personnel. Les traitements sont consignés dans un **registre unique**. Chaque traitement fait l'objet d'une étude documentée permettant de valider sa finalité, sa sécurité, la durée de conservation des données visées. Il est également analysé selon le principe du « privacy by design » Une revue régulière des traitements de données est prévue au sein de chaque direction par les CPD.

3

ANALYSE D'IMPACT

Pour assurer la protection des droits et libertés des personnes

Le CEA a mis en place des procédures d'**analyse systématique de la conformité des traitements** par le DPD et le CPD de la direction concernée par le traitement. Les traitements les plus sensibles font l'objet d'une analyse d'impact sur la vie privée.

4

MESURES TECHNIQUES ET ORGANISATIONNELLES APPROPRIEES AUX TRAITEMENTS

Pour garantir le niveau de sécurité adapté au risque

La **sécurité des données** est inhérente aux activités du CEA. Le Correspondant sécurité à la protection des données (CSPD) est mobilisé pour veiller à la mise en œuvre des mesures techniques et organisationnelles appropriées. Ces mesures sont formalisées dans la Politique de sécurité des systèmes d'information du CEA (PSSI) qui vise à assurer la protection des informations dont le CEA est le propriétaire ou le dépositaire, la continuité et l'intégrité des services de traitement et de transport de l'information, ainsi que la conformité avec la PSSI de l'Etat. Un registre de traitement des violations des données est établi.

5

TRANSPARENCE ET DROITS DES PERSONNES

Pour garantir aux personnes physiques l'accès aux informations clés et la maîtrise de leurs données

Le CEA est attaché à procurer une **information concise et transparente** à toutes les personnes physiques dont il traite les données personnelles, notamment via ses sites intranet, Internet et par voie d'affichage. Un document d'information sur la protection des données à caractère personnel est disponible sur la page du site www.cea.fr dédiée à la protection des données. Par ailleurs, une adresse électronique dédiée - dpd@cea.fr - a été créée pour permettre aux personnes physiques d'**exercer facilement leurs droits sur leurs données**. Ce point d'entrée unique permet de centraliser les demandes et de conserver la trace des réponses apportées. Les collaborateurs du CEA sont régulièrement sensibilisés au respect des droits des personnes.

6

GESTION DU CYCLE DE VIE DE LA DONNEE

De la collecte à son archivage ou sa destruction

Le CEA a établi des règles strictes pour assurer la **protection de la donnée tout au long de sa vie** (en base active, en archive et également au moment de sa destruction). Ces règles sont à la fois techniques et organisationnelles et sont régulièrement revues afin d'assurer une adéquation entre la conservation de la donnée et la finalité pour laquelle elle est traitée. La politique d'archivage des données à caractère personnel du CEA est visée dans une politique interne fondée sur les obligations de l'établissement public au regard du code du patrimoine et du code des relations entre le public et l'administration.

7

GESTION DES TRANSFERTS DE DONNEES

Pour assurer la protection des données transférées

Le CEA a une procédure stricte de **sélection des sous-traitants** et vérifie qu'ils présentent des garanties suffisantes. Le principe est l'hébergement des données à caractère personnel en interne sur le site du CEA. Aucun transfert de données n'est opéré sans que soit définies, par voie contractuelle, leurs conditions d'usage et de sécurité. Les transferts hors Union européenne sont exceptionnels et strictement encadrés.

8

REFERENTIEL INTERNE

Un large référentiel de règles et bonnes pratiques relatives à la protection des données

Le CEA a établi un ensemble de règles internes contribuant à assurer la protection des données personnelles :

- principes et organisation de la protection des données à caractère personnel,
- politique de sécurité des systèmes d'information,
- règlement intérieur de chaque centre du CEA,
- charte d'utilisation des moyens informatiques et des services Internet,
- documents et outils juridiques accessibles sur l'intranet CEA rubrique RGPD.