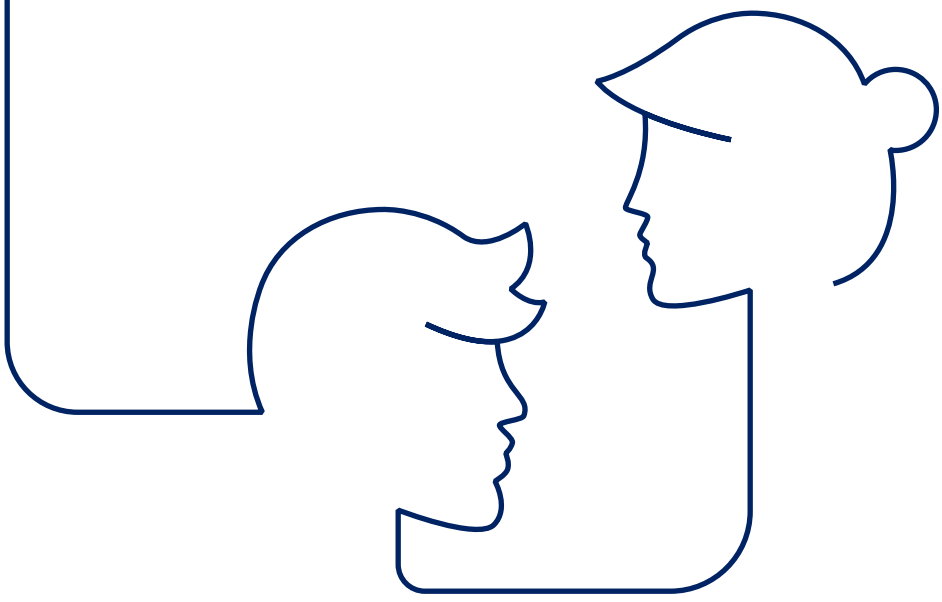
Assurons
un monde
plus ouvert

CNP
assurances

CNP Assurances

Synthèse politique Groupe de protection des données à caractère personnel

23 décembre 2024



Version 2

1. Objet et enjeux

- La protection des données à caractère personnel (DCP) est une obligation légale dans l'UE, notamment avec le RGPD.
- La politique s'applique à toutes les entités du Groupe CNP Assurances, en France et à l'international.
- Elle concerne toutes les personnes dont les DCP sont traitées par le Groupe, y compris les collaborateurs et clients.
- Les principes de cette politique s'appliquent, légalement et/ou par le biais de conventions/contrats, à l'ensemble des sous-traitants du Groupe CNP Assurances y compris aux délégataires et partenaires, ainsi qu'aux fournisseurs.
- La politique prévaut sur les règles locales si elles sont moins exigeantes.
- Si la législation locale prévoit des dispositions supplémentaires, celles-ci sont intégrées aux dispositifs locaux.
- Les modifications ou adaptations locales de la politique doivent être validées par le DPOG.
- La politique s'applique à tous les formats de DCP, papier ou électronique.
- Les traitements de DCP doivent respecter des obligations spécifiques selon les lois locales.
- La protection des DCP est essentielle pour la confiance des clients et la réputation du Groupe.
- Cette politique est revue a minima annuellement.

2. Principes fondamentaux de protection des DCP

- Les DCP doivent être traitées de manière licite, loyale et transparente.
- Elles doivent être collectées pour des finalités déterminées et légitimes.
- Les DCP doivent être adéquates, pertinentes et limitées aux finalités du traitement.
- Elles doivent être exactes et tenues à jour.
- Les DCP doivent être conservées pendant une durée définie et sécurisées. CNP Assurances a en effet défini des référentiels de durées de conservation.
- Le Groupe doit démontrer sa conformité avec les réglementations de protection des DCP.
- La protection des DCP doit être intégrée dès la conception des projets (*Privacy by Design*).
- Une analyse de risque sur la vie privée doit être réalisée pour tout nouveau traitement de DCP ou de toute modification de traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques concernées
- Un registre des traitements de DCP doit être maintenu et mis à jour.
- Les relations avec les tiers doivent inclure une évaluation de leurs mesures de protection des DCP.

3. Gouvernance de la protection des DCP

- Chaque entité du Groupe est responsable de la protection des DCP qu'elle traite.
- Le Groupe met en place une filière de protection des DCP avec des rôles et responsabilités définis.
- Le DPOG est responsable de la protection des DCP au niveau du Groupe.
- Les DPOFS sont responsables au niveau des filiales et succursales.
- Des correspondants peuvent être nommés pour gérer les traitements de DCP au sein des entités.
- Les autres acteurs (responsables métiers, RSSI, etc.) ont des rôles spécifiques dans la protection des DCP.
- Les instances dirigeantes et les correspondants se réunissent périodiquement pour discuter de la protection des DCP.
- En cas de désaccord, l'arbitrage est traité par la voie hiérarchique et, le cas échéant, par le Directeur Général de CNP Assurances ou de l'entité concernée.
- Un plan de contrôle et d'audit interne sur la protection des DCP doit être mis en œuvre.
- Un processus est mis en place visant à permettre l'identification des violations de DCP, leur correction et la mise en place de plans d'actions préventifs qui sont suivis. Les violations de DCP sont également, en cas d'impacts importants pour les personnes concernées, notifiées à la CNIL et/ou aux personnes concernées.
- Il est à noter que CNP Assurances ne fournit pas, ni ne loue, ni ne vend de données à caractère personnel à des tiers pour des raisons autres que celles nécessaires au bon traitement des opérations. De même, CNP Assurances ne collecte pas elle-même de données auprès des tiers/partenaires hormis celles nécessaires au bon traitement des opérations.

4. Sensibilisations

- Les collaborateurs doivent être périodiquement sensibilisés à la protection des DCP.
- La formation doit inclure les exigences réglementaires et les risques liés aux DCP.
- Les modules de sensibilisation doivent être adaptés à la législation locale.
- La formation peut être réalisée par e-learning, en présentiel ou lors d'événements externes.
- Un plan de formation sur la protection des DCP doit être mis en place.
- Les campagnes de sensibilisation doivent être déployées au sein du Groupe.
- Les collaborateurs doivent comprendre les règles de collecte et d'utilisation des DCP.
- Les informations sur l'organisation de la filière de protection des DCP doivent être partagées.

5. Reporting et contrôle

- Les reportings sont réalisés par les correspondants, les DPOFS et le DPOG.
- Le DPOG consolide les reportings et les présente aux instances dirigeantes du Groupe CNP Assurances, de la Caisse des dépôts et Consignations et de La Banque Postale.
- Un plan de contrôle sur la protection des DCP doit être mis en œuvre par les entités.
- Les contrôles doivent être basés sur la législation locale et les exigences du Groupe.
- L'efficacité des contrôles est autoévaluée chaque année par ceux qui les mettent en œuvre et, le contrôle permanent effectue des tests périodiques pour s'assurer que les autoévaluations sont le reflet de la réalité.
- L'audit interne intègre le contrôle de la protection des DCP dans son plan d'audit périodique.
- Des audits des délégataires sont également réalisés avec un volet sur la protection des données à caractère personnel. Les délégataires critiques et importants sont audités tous les ans et le reste du périmètre de manière périodique et en fonction du résultat de l'audit précédent (si l'audit précédent n'est pas satisfaisant, un audit aura lieu de façon plus régulière). Ces audits se déroulent via 2 phases :
  - la première avec l'envoi d'un questionnaire aux délégataires sur le Règlement Général de la Protection des Données (question sur la gouvernance, les obligations réglementaires, la description des traitements effectués, la formation des collaborateurs, etc.),
  - la seconde via un entretien d'audit d'une heure sur ce sujet avec la Direction de la Conformité du délégataire audité.
- Les audits externes de sécurité informatique des prestataires intègrent une partie sur la protection des données à caractère personnel.
- Le Groupe collabore avec les autorités de contrôle pour toute question relative aux DCP.
- Les processus doivent permettre de se conformer aux recommandations des autorités de contrôle.
- Les DPOG/DPOFS sont les interlocuteurs privilégiés des autorités de contrôle.
- L'autorité de contrôle "chef de file" pour le Groupe est la CNIL en France.

6. Déclinaison de la présente politique

- La politique se décline dans un référentiel opérationnel comprenant des procédures et une matrice des rôles et responsabilités.
- Ce référentiel est mis à disposition des entités du Groupe pour une adaptation locale.

.

Assurons
un monde
plus ouvert

CNP Assurances – Siège social : 4 promenade Cœur de Ville 92130 Issy-les-Moulineaux – 01 42 18 88 88 – www.cnp.fr
Société anonyme au capital de 686 618 477 euros entièrement libéré – 341 737 062 RCS Nanterre
Entreprise régie par le code des assurances – IDU EMP FR231782_01ZWUC