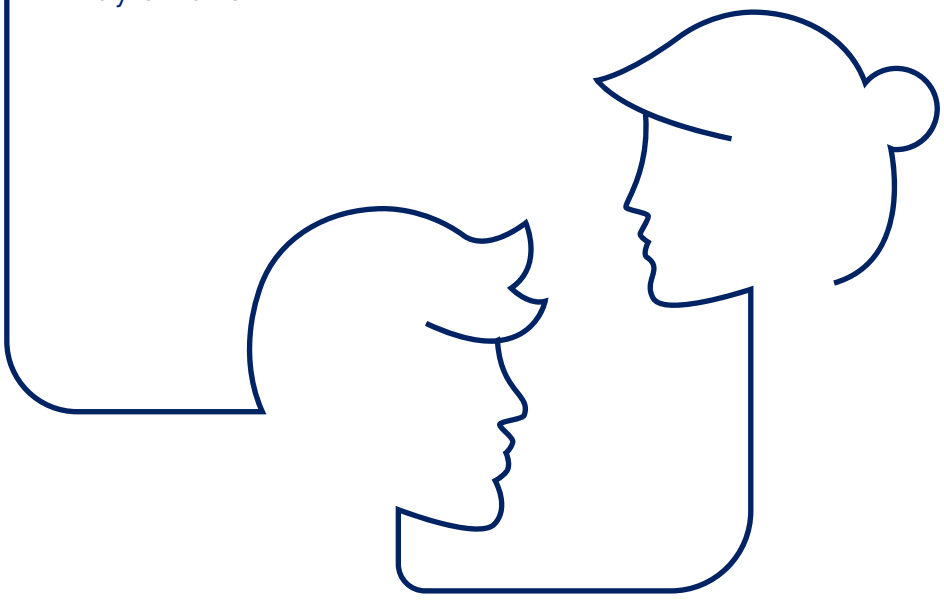
Insuring
a more
open world

CNP
assurances

CNP Assurances

Summary of the Group policy on personal data protection

May 6 2026



Version 4

1. Purpose and key issues

- Data privacy is a legal obligation within the EU, particularly under the GDPR (General Data Protection Regulation).
- This policy applies to all entities of the CNP Assurances Group, both inside and outside of the European Union.
- It concerns all individuals whose personal data is processed by the Group, including employees and clients (ie the data subjects).
- A framework procedure governs all activities of the Business Units and Group functions of CNP Assurances.
- The principles of this policy apply—either by law or through agreements/contracts—to all of the Group's subcontractors, including its delegatees, partners, and suppliers.
- This policy takes precedence over local regulations if those are less stringent.
- If local legislation includes additional provisions, they are incorporated into local policy.
- Any local modifications or adaptations of this policy must be approved by the Group Data Protection Officer (GDPO).
- The policy applies to all personal data, whether collected in paper or electronic form, directly by CNP Assurances or indirectly through its partners and processors, from policyholders or prospective policyholders.
- The collection of personal data is necessary to carry out underwriting and to ensure the proper management of policyholders' contracts.
- In addition to the authorised staff of CNP Assurances, other parties may have access to personal data, also for the purposes of underwriting and the proper management of contracts, including our service providers, partners, processors, reinsurers and, where applicable, the social security bodies of the individuals concerned, insurance intermediaries, as well as parties with an interest in the contract.
- Personal data processing must comply with specific obligations under local laws.
- Data privacy is essential to maintain client trust and protect the Group's reputation.
- This policy is reviewed at least annually.

2. Core principles of personal data protection

- Personal data must be processed lawfully, fairly, and transparently.
- It must be collected for specific and legitimate purposes.
- Personal data must be adequate, relevant, and limited to what is necessary for the intended processing purposes.
- It must be accurate and kept up to date.
- CNP Assurances has implemented a personal data retention policy and a personal data retention procedure.
- Personal data must be retained for a defined period and secured accordingly. CNP Assurances has established reference standards for retention periods.
- The Group must be able to demonstrate its compliance with personal data protection regulations.
- The Group implements appropriate technical and organisational measures, both by design and by default, to ensure the protection of personal data. In this context, dedicated internal tools have been developed to ensure these measures are embedded in every project. As part of a continuous innovation approach, particular attention has been paid to processing of personal data involving Artificial Intelligence (AI) systems, in order to anticipate and manage the specific risks associated with AI systems from the design stages.
- A privacy risk assessment must be conducted for any new personal data processing or any modification of an existing processing likely to give rise to a high risk to the rights and freedoms of the natural data subjects.
- A register of personal data processing activities must be maintained and regularly updated.
- Relationships with third parties must include an evaluation of their personal data protection measures.
- The Group entities handle all requests to exercise data subject rights, particularly the rights of access, deletion, objection and rectification of data subjects' personal data, within one month, or within three months in the case of complex requests, in accordance with applicable regulations and subject to any more stringent national rules. Data subjects may exercise their rights at any time by submitting their request by any means, for example by email, by postal mail, or by completing an online request form. If a deletion request is granted, any backup copy of the data shall also be permanently deleted within 60 days following its deletion from the active database.

3. Governance of personal data protection

- Each entity within the Group is responsible for protecting the personal data it processes.
- The Group has established a personal data protection governance with defined roles and responsibilities.
- The Group Data Protection Officer (GDPO) is responsible for personal data protection at the Group level.
- Subsidiary or Branch Data Protection Officers (DPOFS) are responsible for personal data protection at their respective subsidiaries and branches levels.
- The Audit and Risk Committee (ARC), composed of Group board members, provides regular oversight of issues relating to personal data security.
- Correspondents ("Relais Informatique et Libertés" (RILs) in France or Privacy Champions) may be appointed within entities to manage personal data processing activities.
- Other stakeholders (business managers, Chief Information Security Officers, etc.) have specific roles in ensuring personal data protection.
- Governing bodies and correspondents meet periodically to discuss personal data protection matters.
- In case of disagreement, the arbitration is handled through the hierarchical chain and, if necessary, by the Chief Executive Officer of CNP Assurances or the relevant entity.
- An internal control and audit plan for personal data protection must be implemented.
- A process is in place to identify personal data breaches, correct them, and implement preventive action plans that are monitored. In cases where personal data breaches significantly impact the data subjects, notifications are made to the French data protection authority (CNIL) and/or the affected data subjects.
- The Group respects the rights of data subjects. Group entities implement the necessary measures to respond as promptly as possible to data subjects, thereby enabling them to exercise the rights provided under the GDPR, including the rights of access, rectification, and deletion, while taking into account applicable legal provisions.
- It should be noted that CNP Assurances does not provide, rent, or sell personal data.
- Data privacy is embedded within CNP Assurances Group's risk and compliance management framework. A risk and control mapping process incorporates key issues related to personal data protection, in accordance with the requirements of the GDPR.

4. Awareness and training

- Employees, including part-time staff, must be periodically made aware of personal data protection requirements.
- Training should cover regulatory obligations and the risks associated with personal data.
- Awareness modules must be tailored to local legislation.
- Training may be delivered via e-learning, in-person sessions, or external events.
- A formal training plan on personal data protection must be rolled out.
- Awareness campaigns must be implemented across the Group.
- Employees must understand the rules governing the collection and use of personal data.
- Information about the organization of the personal data protection governance within the Group must be shared.
- Service providers must also ensure that persons authorised to process personal data commit to confidentiality, or are subject to an appropriate legal obligation of confidentiality, and receive the necessary training in the protection of personal data. Service providers undertake to make available to CNP Assurances the evidence required to demonstrate compliance with this obligation.

5. Reporting and control

- Reporting is carried out by Correspondents/Privacy Champions, DPOFS (Data Protection Officers for Subsidiaries and Branches), and the Group Data Protection Officer (GDPO).
- The GDPO consolidates the reports and presents them to the executive bodies of CNP Assurances Group, the Caisse des Dépôts et Consignations, and La Banque Postale.
- Each entity must implement a control plan for personal data protection.
- Controls must be based on both local legislation and Group requirements.
- The effectiveness of controls is self-assessed annually by those responsible for implementation, and permanent control team conducts periodic tests to ensure that self-assessments reflect reality.
- Internal audit includes personal data protection in its periodic audit plan.

- Audits of delegatees also include a section on personal data protection. Critical and major delegatees are audited annually, while others are audited periodically based on the results of previous audits (if the previous audit was not satisfactory, audits will be conducted more frequently). These audits consist of two phases :
    - The first involves sending a questionnaire to delegatees regarding the General Data Protection Regulation (questions on governance, regulatory obligations, description of processing activities, employees training, etc.).
    - The second consists of a one-hour audit interview on this topic with the Compliance Department of the audited delegatee.
- External IT security audits of service providers include a section on personal data protection.
- Audits are conducted with our partners and suppliers to verify their compliance with the GDPR, particularly regarding the existence and implementation of a privacy policy.
- CNP Assurances has been subject to external audits, including by its parent company, La Banque Postale.
- The Group collaborates with supervisory authorities on all matters related to personal data.
- Processes must enable compliance with recommendations issued by supervisory authorities.
- The GDPO and DPOFS serve as the primary contacts for supervisory authorities.
- The lead supervisory authority for the Group is the CNIL in France.

6. Implementation of this policy

- This policy is supported by an operational framework that includes procedures and a roles and responsibilities matrix.
- This framework is made available to Group entities for local adaptation.

Insuring
a more
open world

CNP Assurances – Registered office: 4, promenade Cœur de Ville 92130 Issy-les-Moulineaux – Tel.: +33 (0)1 42 18 88 88 – www.cnp.fr
Société anonyme (joint-stock company) with fully paid-up share capital of €686,618,477 Registered in the Nanterre Trade and Companies Register under no. 341 737 062 – Company governed by the French Insurance Code (Code des assurances) – IDU EMP FR231782_01ZWUC