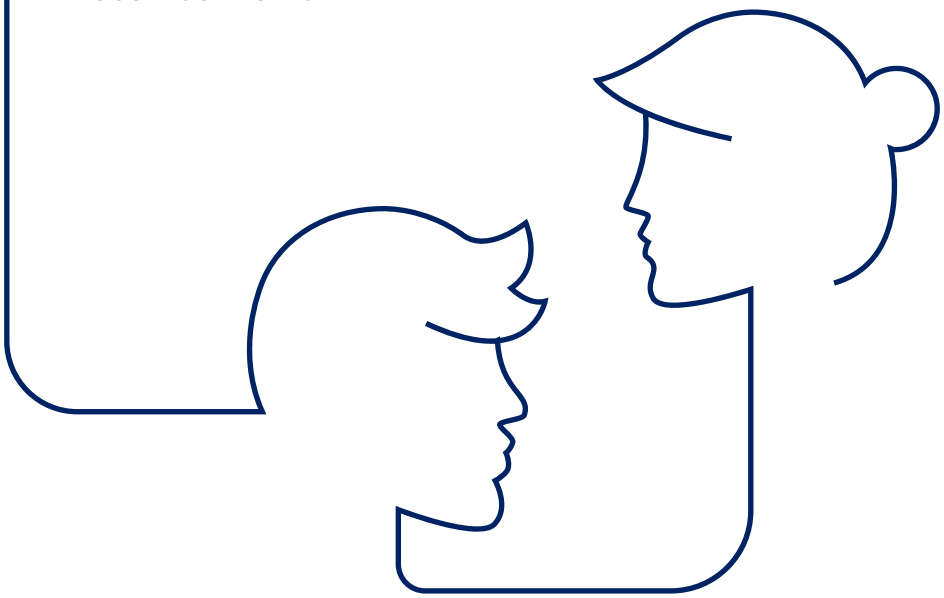
Insuring
a more
open world

CNP
assurances

CNP Assurances

Summary of the Group policy on personal data protection

December 23 2024



Version 2

1. Purpose and key issues

- Data Protection (DP) 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).
- 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 formats of personal data, whether paper-based or electronic.
- Personal data processing must comply with specific obligations under local laws.
- Protecting personal data is essential to maintaining client trust and safeguarding 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.
- Personal data must be retained for a defined period and secured accordingly. CNP Assurances has established retention periods repositories.
- The Group must be able to demonstrate its compliance with personal data protection regulations.
- Data protection must be embedded from the design phase of any project (Privacy by Design).
- 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 individuals concerned.
- 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.

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 .
- 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.
- It should be noted that CNP Assurances does not provide, rent, or sell personal data to third parties for purposes other than those required for proper operational processing. Similarly, CNP Assurances does not collect data from third parties/partners except when necessary for operational processing.

4. Awareness and training

- Employees 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 implemented.
- Awareness campaigns must be deployed 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.

5. Reporting and control

- Reporting is carried out by Correspondents, 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.
- 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