✅ ChecklistGuro

Insurance Data Privacy Compliance Checklist

Data Inventory & Mapping

Identify and document personal data collected, processed, and stored related to insurance customers and applicants.

Description of Data Collected (e.g., Name, Address, DOB, Medical History)

Write something...

Data Category (e.g., Personally Identifiable Information, Financial Data, Medical Information)

☐ Personally Identifiable Information (PII)

☐ Financial Data

☐ Medical Information

☐ Behavioral Data

☐ Location Data

Approximate Number of Records Containing This Data

Enter a number...

Data Source (e.g., Application Form, Website, Third-Party Provider)

☐ Application Form

☐ Website

☐ Third-Party Provider

☐ Claims Data

Date Data Inventory Last Updated

Enter date...

Data Retention Policy (Summary)

Write something...

Consent & Notices

Verify compliance with consent requirements for data collection, use, and sharing. Review and update privacy notices.

Consent Method Used

☐ Explicit Opt-In

☐ Implied Consent

☐ Legitimate Interest (Documented)

Summary of Privacy Notice Content

Write something...

Last Privacy Notice Update Date

Enter date...

Copy of Current Privacy Notice (PDF)

⬆ Upload File

Notice Delivery Method

☐ Website

☐ Email

☐ Paper Form

☐ Pre-contractual Information

Description of Consent Withdrawal Process

Write something...

Number of Consent Withdrawal Requests Processed Last Year

Enter a number...

Data Subject Rights Requests (DSRs)

Establish and test procedures for handling data subject access requests, rectification requests, erasure requests, and restriction of processing requests.

Date of DSR Received

Enter date...

DSR Reference Number (Internal)

Write something...

Details of DSR Request (Customer's Exact Words)

Write something...

Type of DSR Requested

☐ Access

☐ Rectification

☐ Erasure

☐ Restriction of Processing

☐ Data Portability

☐ Objection

Number of Records/Data Points Involved (Estimate)

Enter a number...

Date of Acknowledgement Sent to Customer

Enter date...

Summary of Actions Taken to Address DSR

Write something...

Date DSR Fully Resolved

Enter date...

Resolution Status

- [ ] Fully Resolved
- [ ] Partially Resolved
- [ ] Denied (with Explanation)

Reason for Denial (if applicable)

Write something...

Data Security Measures

Assess and verify technical and organizational security measures to protect personal data, including encryption, access controls, and data loss prevention.

Encryption Strength (Bit Length)

Enter a number...

Encryption Type Used (e.g., AES, RSA)

- ☐ AES
- ☐ RSA
- ☐ Other - Specify in Long Text

Access Control Measures Implemented

- ☐ Role-Based Access Control
- ☐ Multi-Factor Authentication
- ☐ Least Privilege Principle
- ☐ Regular Access Reviews

Firewall Status

- ☐ Active
- ☐ Inactive
- ☐ Pending Review

Last Penetration Test Date

Enter date...

Description of Data Loss Prevention (DLP) measures

Write something...

Third-Party Vendor Management

Evaluate and monitor third-party vendors' data privacy practices and contractual obligations.

Vendor's Privacy Framework Alignment (e.g., SOC 2, ISO 27001)

- [ ] Fully Compliant
- [ ] Partially Compliant
- [ ] Not Compliant
- [ ] N/A

Summary of Vendor's Data Processing Activities

Write something...

Vendor's Data Processing Agreement (DPA)

⬆ Upload File

Vendor's Security Assessment Completion Status

- [ ] Completed
- [ ] In Progress
- [ ] Not Completed

Last Vendor Security Assessment Date

Enter date...

Number of Records Processed by Vendor (Estimate)

Enter a number...

Description of Vendor's Data Security Controls

Write something...

Data Breach Response Plan

Review and test the data breach response plan to ensure timely and effective response to data breaches.

Last Breach Response Plan Review Date

Enter date...

Summary of Breach Response Plan

Write something...

Primary Contact Person for Data Breach

☐ Name 1

☐ Name 2

☐ Name 3

Secondary Contact Person for Data Breach

☐ Name 1

☐ Name 2

☐ Name 3

Estimated Cost of a Data Breach (USD)

Enter a number...

Description of Data Breach Containment Steps

Write something...

Incident Report Template (Example)

⬆ Upload File

Training and Awareness

Confirm completion of data privacy training for relevant employees and contractors.

Number of Employees Trained

Enter a number...

Last Training Completion Date

Enter date...

Training Modules Covered (Select All)

☐ Data Subject Rights (DSRs)

☐ Data Security Practices

☐ Privacy Policy Updates

☐ Incident Reporting

☐ Vendor Management

Training Delivery Method

☐ Online Module

☐ Classroom Training

☐ Webinar

Summary of Training Content

Write something...

Training Completion Certificates

⬆ Upload File

Regulatory Updates

Track and implement changes to applicable data privacy laws and regulations (e.g., GDPR, CCPA, state-specific laws).

Date of Last Regulatory Update Review

Enter date...

Summary of Regulatory Changes Identified

Write something...

Applicable Regulations (Select All)

- [ ] GDPR
- [ ] CCPA
- [ ] HIPAA
- [ ] State-Specific Privacy Laws
- [ ] Other (Specify in Long Text)

Details of 'Other' Regulations Selected (If Applicable)

Write something...

Implementation Deadline for New Requirements

Enter date...

Number of Employees Trained on New Regulations

Enter a number...

Status of Implementation

- ☐ Not Started
- ☐ In Progress
- ☐ Completed
- ☐ Delayed

Policy and Procedure Review

Regularly review and update data privacy policies and procedures to reflect legal changes and business practices.

Last Policy Review Date

Enter date...

Summary of Changes Made During Last Review

Write something...

Review Scope (e.g., Full, Targeted)

- ☐ Full Review
- ☐ Targeted Review

Review Cycle Frequency (e.g., Annual, Bi-annual)

Enter a number...

Description of process used to identify relevant regulatory updates

Write something...

Supporting Documentation (e.g., Review Reports)

⬆ Upload File

Data Transfer Compliance

Verify compliance with international data transfer mechanisms (e.g., Standard Contractual Clauses, Binding Corporate Rules) if transferring data outside of relevant jurisdictions.

Data Transfer Mechanism Utilized

☐ Standard Contractual Clauses (SCCs)

☐ Binding Corporate Rules (BCRs)

☐ Adequacy Decision

☐ Other (Specify in LONG_TEXT)

If 'Other' selected, specify the data transfer mechanism.

Write something...

Date SCCs/BCRs were last reviewed/updated.

Enter date...

Number of countries data is transferred to.

Enter a number...

Countries Data is Transferred To (Select all that apply)

☐ United States

☐ United Kingdom

☐ Canada

☐ Australia

☐ Germany

☐ France

☐ Japan

☐ Other (Specify in LONG_TEXT)

If 'Other' selected above, specify countries.

Write something...

Upload Copy of SCCs/BCRs or Transfer Impact Assessment

⬆ Upload File