

CRM Data Privacy Checklist

Data Subject Rights Compliance

Ensuring processes are in place to handle data subject requests (access, rectification, erasure, restriction, portability).

Number of Data Subject Access Requests Received (Last 3 Months)

Last Data Subject Access Request Received

Process for Verifying Identity of Data Subject

- Manual Verification
- Automated Verification
- Combination of Both

Summary of Processes for Responding to Rectification Requests

Deadline for Responding to Data Subject Requests (e.g., under GDPR)

Enter date...

Record of Exceptions to Data Subject Rights (e.g., legal obligations)

Write something...

Consent Management

Verifying proper consent mechanisms for data collection and processing are implemented and documented.

Consent Collection Method

- Online Form
- Paper Form
- Verbal Consent

Last Consent Review Date

Enter date...

Description of Consent Language Used

Write something...

Types of Data Requiring Consent

- Name
- Email Address
- Phone Number
- Location Data
- Purchase History

Consent Recording Method

- CRM System
- Separate Consent Management Platform
- Manual Recording

Estimated Percentage of Users Providing Consent

Enter a number...

Data Minimization

Confirming only necessary data is collected and stored within the CRM.

Identify redundant data fields

- Yes, reviewed and identified
- No, not yet reviewed

Number of data fields identified for removal/modification

Enter a number...

Justification for retaining any potentially unnecessary fields

Write something...

Are default values implemented to minimize data entry?

- Yes, implemented for key fields
- Partially implemented
- No, not implemented

Are imported data fields reviewed for necessity?

- Yes, standard practice
- Sometimes
- No

Purpose Limitation

Validating data is used only for specified, legitimate purposes and documented accordingly.

Describe the Primary Purpose(s) for CRM Data Collection

Write something...

Does the CRM data usage align with the declared purpose?

- Yes
- No
- Not Applicable

Number of data usage purposes documented

Enter a number...

Explain any Secondary Uses of Data and Justification

Write something...

Is there documented approval for secondary data usage?

- Yes
- No
- Not Applicable

Describe processes to ensure data is not used for unintended purposes

Write something...

Data Security Measures

Assessing the effectiveness of security controls (encryption, access restrictions, data loss prevention).

Encryption Strength (in bits)

Enter a number...

Data at Rest Encryption Enabled?

- Yes
- No
- Not Applicable

Data in Transit Encryption Protocol (TLS/SSL)

- TLS 1.2
- TLS 1.3
- SSL (Deprecated - Not Recommended)

Access Control Measures Applied?

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

Firewall Configuration?

- Standard Configuration
- Custom Configuration
- Not Applicable

Description of Security Audits Conducted (Date, Findings)

Write something...

Third-Party Vendor Management

Reviewing contracts and data processing agreements with third-party vendors.

Vendor DPA (Data Processing Agreement) Status

- DPA Signed
- DPA Drafted
- No DPA in Place

DPA Expiration Date

Enter date...

Summary of Vendor's Security Practices

Write something...

Number of Sub-Processors Used by Vendor

Enter a number...

Security Audit Reports Received from Vendor?

- SOC 2
- ISO 27001
- Other
- No Audit Reports Received

Vendor Security Questionnaire Response

 Upload File

Data Retention Policies

Ensuring data is retained only as long as necessary and securely disposed of afterward.

Retention Period (Years)

Enter a number...

Data Type(s) Subject to Retention

- Contact Information
- Sales History
- Marketing Interactions
- Support Tickets
- All Data

Last Review Date of Retention Schedule

Enter date...

Justification for Retention Period(s)

Write something...

Data Destruction Method

- Secure Deletion
- Data Sanitization
- Physical Destruction

Date of Next Retention Schedule Review

Enter date...

Data Breach Response Plan

Reviewing and testing the plan for responding to data breaches and notifying relevant parties.

Incident Description (Initial Report)

Write something...

Date of Breach Detection

Enter date...

Time of Breach Detection

Breach Severity (Low, Medium, High)

Low

Medium

High


Estimated Number of Records Affected

Enter a number...

Containment Steps Taken

Write something...

Supporting Documentation (e.g., screenshots, logs)

 Upload File

Date of Notification to Data Protection Authority (if applicable)

Enter date...

Legal and Regulatory Compliance

Verifying adherence to applicable privacy laws (e.g., GDPR, CCPA, HIPAA).

Applicable Privacy Laws

- GDPR
- CCPA/CPRA
- HIPAA
- PIPEDA
- Other (Specify in Long Text)

Specific Legal Requirements

Write something...

Last Compliance Review Date

Enter date...

Number of Data Processing Agreements (DPAs)

Enter a number...

Data Transfer Mechanisms (if applicable)

- Standard Contractual Clauses (SCCs)
- Binding Corporate Rules (BCRs)
- Adequacy Decision
- Other (Specify in Long Text)

Documentation of Legal Basis for Processing

Write something...

Training and Awareness

Ensuring employees are trained on data privacy best practices and CRM responsibilities.

Topics Covered in CRM Privacy Training

- Data Subject Rights
- Consent Management
- Data Security
- Incident Reporting
- Legal & Regulatory Framework

Number of Employees Trained

Enter a number...

Last Training Session Date

Enter date...

Training Delivery Method

- Online Module
- Classroom Session
- Hybrid

Summary of Training Content

Write something...

Training Material Version

- v1.0
- v1.1
- v2.0