Data Retention & Disposal Policy

Introduction

This Data Retention Policy has been adopted by Anteriad in order to set out the principles for retaining personal data. This Policy covers all personal data held by Anteriad, personal data that was processed by telemarketing, email marketing or through visiting Anteriad's website.

This Policy should be read in conjunction with other policies that have as their objectives the protection and security of data such as the Anteriad Privacy Policy.

Purpose

This Data Retention Policy establishes rules for the retention, storage, and disposal of personal and business data in compliance with:

- **Europe:** General Data Protection Regulation (GDPR), ePrivacy Directive, and applicable Member State laws.
- **United States:** Federal and state laws, including but not limited to HIPAA, SOX, SEC, FINRA, and CCPA/CPRA.

The goal is to balance legal obligations, business needs, and individuals' privacy rights.

Scope

This policy applies to:

- All employees, clients, contractors, and third-party vendors handling company data.
- All formats of data (electronic, paper, audio, video).
- All jurisdictions where the organization operates.

Principles

- **Data Minimization (EU & US):** Only retain data that is necessary for the specified purpose.
- **Storage Limitation (GDPR Art. 5):** Data must not be kept longer than required.
- **Legal Compliance:** Retention periods must comply with sector-specific laws.
- **Right to Erasure (EU):** Individuals may request deletion of personal data when retention is no longer justified.
- **Litigation Hold (US):** Data relevant to ongoing or potential litigation must be preserved, regardless of standard retention periods.

Retention of personal data

Anteriad will retain the collected personal information for the period necessary to fulfil the purposes, that was expressly explained while the data was collected (by email, phone conversation, email marketing or by visiting our website).

Any personal data collected by Anteriad operators will be US and GDPR compliant because of following the “transparency-consent-traceability” methodology. All the data subjects will know what data will be saved by Anteriad and for which purpose.

All the information that will be collected, other than personal information, will be stored for the duration of the marketing relationship and sent to the client, if applicable, in the delivery. By information, we refer to any points of data that was collected or (by email, phone conversation, email marketing or by visiting our website) that were discussed during the communication about technical issues or IT related information, that are necessary for the Clients.

All the collected personal information will be held in our secured servers for a limited period to fulfil the purpose.

These servers will be accessible only by a few of Anteriad employees, that will have the right to access to the data. The servers are AWS Cloud based out of the US and Azure Cloud based out of Paris.

Data Retention & Schedule

Data Category	Retention Period	Legal / Business Basis	Action After Expiry
Client-supplied customer lists & contact data	Maximum 24 months after last campaign/use, unless consent requires earlier deletion	GDPR storage limitation; PECR consent rules	Secure electronic deletion
Marketing Data (consent)	Until consent withdrawn or 2 years inactivity	Consent (Art. 6(1)(a))	Delete
Emails & Communications	3–7 years depending on sensitivity	Legitimate interest / compliance	Delete
Customer Records	Active relationship + 5 years	Contractual / legal	Delete or anonymize
Contracts/Agreements	Term + 6 years	Limitation periods	Archive then delete
Campaign creative assets (artwork, ads, copy, design files)	3 years after project completion (unless contract specifies longer)	Contractual IP/licensing rights may require retention	Secure deletion or shredding

Campaign reports & analytics	3 years after delivery to client	Retained for audit & performance verification	Secure Deletion
Temporary working files (drafts, test data, staging versions)	Deleted immediately once final deliverables approved	Best practice (no legal requirement)	Secure Deletion
Employee HR Records	6 years after termination	Employment law	Delete or anonymize
Recruitment Applications	12 months (unless consent given)	Legitimate interest	Delete
Payroll & Tax Records	6 years	Tax & accounting law	Secure archive then delete
Health & Safety Records	5–40 years	Legal obligations	Delete securely
CCTV / Surveillance	30 days (unless incident)	Legitimate interest	Automatic overwrite
Website/Analytics Data	12–24 months	Consent / legitimate interest	

Data Deletion and Disposal

- **Electronic Data:** Secure erasure methods (e.g., data wiping, encryption destruction).
- **Physical Records:** Shredding or incineration.
- **Documentation:** Maintain logs of deletion activities for compliance audits.

Exceptions

- Data subject requests for erasure (GDPR) will be honored unless legal obligations require continued retention.
- US litigation holds override scheduled deletion until resolution.

Roles & Responsibilities

- **Data Protection Officer (DPO) (EU) / Privacy Officer (US):** Oversees compliance with applicable laws.
- **IT & Security Teams:** Implement secure retention and deletion processes.
- **Department Heads:** Ensure staff follow the retention schedule.

Review and Updates

- Policy will be reviewed annually or in response to regulatory changes in either jurisdiction.
- Retention schedules will be updated accordingly.