

Data Management & Purge Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Version: 1.2

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

Document Revision History:

VERSION NO.	REVISION DATE	AUTHOR	REVIEWED BY	APPROVED BY	DESCRIPTION
1	28/6/2022	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed
1.1	28/6/2023	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed
1.2	28/7/2024	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed

Purpose

This Data Management Policy establishes guidelines for managing, storing, and accessing data within **BPO Convergence Pvt.Ltd.** As a call center, this policy addresses compliance with industry standards, legal requirements, and operational needs. It specifically outlines practices for Call Detail Records (CDRs), CRM reports, and call recordings to maintain data integrity, confidentiality, and accessibility.

Scope

This policy applies to all employees, contractors, and third-party entities who handle, access, or manage data within **BPO Convergence Pvt.Ltd.** It includes electronic records stored on servers and any backups or archival systems.

Policy Statements

1. Data Retention

1.1 Retention Periods:

- **Call Detail Records (CDRs):** Retain for 180 days on the server.
- **CRM Reports:** Maintain reports for 7 days for operational and audit purposes.
- **Call Recordings:** Store recordings securely for 1 year to meet regulatory and quality assurance requirements.

1.2 Archival and Disposal:

- Archive CDRs and CRM reports exceeding the 180-day limit, ensuring they are securely deleted afterward.
- Automatically remove call recordings older than 1 year unless flagged for legal or operational use.

1.3 Legal and Audit Holds:

- Suspend deletion of data if it is subject to a legal hold, regulatory requirement, or ongoing investigation.

2. Data Storage

2.1 Storage Locations:

- **Primary Storage:** CDRs, CRM reports, and call recordings are stored on secure servers with controlled access.
- **Backup Storage:** Create encrypted backups of critical data weekly, stored at an offsite location.

2.2 Security Measures:

- Encrypt sensitive data, including CDRs and call recordings, during storage and transmission.
- Implement firewalls, intrusion detection systems (IDS), and anti-virus solutions for server security.

2.3 Storage Monitoring:

- Monitor storage usage and performance weekly to ensure sufficient capacity and optimal operation.
- Conduct periodic audits to validate compliance with retention and security protocols.

3. Data Access

3.1 Access Rights:

- Access to CDRs, CRM reports, and call recordings is role-based.
- Supervisors and quality assurance teams have read-only access to recordings for reviews and audits.

3.2 Authentication and Authorization:

- Use multi-factor authentication (MFA) for all users accessing servers containing sensitive data.
- Regularly review and update access permissions to ensure alignment with job roles.

3.3 Audit Trails:

- Maintain detailed logs of data access, retrieval, and modifications for a minimum of 12 months.
- Review logs quarterly to identify unauthorized activities or anomalies.

Compliance and Enforcement



Non-compliance with this policy may lead to disciplinary actions, including termination of employment or contractual agreements. Incidents of non-compliance must be reported to the [IT Security Team or Data Management Team] immediately.

Review and Updates

This policy will be reviewed annually or sooner if required by changes in regulations or business needs.