

Data Privacy & GDPR Policy

Version: 2025-01

Company: [NMT]

Effective Date: [06/12/2025]

Review Date: [06/12/2025]

1. Purpose & Scope

This Data Privacy & GDPR Policy outlines [Company Name]'s commitment to protecting personal data in compliance with data protection laws, including the GDPR. It applies to all employees, contractors, candidates, and customers across global operations, including those within the EU.

2. Key Principles

- 1. Lawfulness, Fairness, and Transparency**
 - 2. Purpose Limitation**
 - 3. Data Minimization**
 - 4. Accuracy**
 - 5. Storage Limitation**
 - 6. Integrity and Confidentiality**
 - 7. Accountability**
-

3. Roles & Responsibilities

- **Data Controller**
 - **Data Processor**
 - **Data Protection Officer (DPO)**
 - **Human Resources (HR)**
 - **Information Technology (IT)**
 - **Managers**
 - **Employees**
-

4. Lawful Bases for Processing

- 1. Contract**
- 2. Legal Obligation**
- 3. Vital Interests**
- 4. Public Interest**
- 5. Legitimate Interests**
- 6. Consent**

Examples:

- Payroll processing (**Contract**)
 - Tax retention (**Legal Obligation**)
 - Promotional emails (**Consent**)
-

5. Data Subject Rights

- 1. Right of Access**
- 2. Right to Rectification**
- 3. Right to Erasure**
- 4. Right to Restriction**
- 5. Right to Data Portability**
- 6. Right to Object**

Handling Timelines:

- Acknowledge within 5 business days
 - Respond within 30 days
-

6. DSAR / Request Handling Process

- 1. Intake**
- 2. Verification**
- 3. Response**

SLA:

- Acknowledge in 5 days
- Fulfill in 30 days

7. Data Classification & Handling Rules

- **Personally Identifiable Information (PII)**
- **Special Categories**
- **Confidential Data**

Handling Rules:

- **Encrypt PII**
 - **Apply heightened security for special categories**
 - **Need-to-know access for confidential data**
-

8. Data Collection & Use

Used during recruitment, payroll, performance management, and security monitoring.

9. Retention & Deletion

9.1 Retention Schedule

Data Category	Retention Period
Employee Records	7 years post-employment
Candidate Applications	1 year
Payroll Data	7 years
Performance Reviews	3 years

9.2 Deletion Methods

- **Secure electronic deletion**
 - **Shredding physical documents**
-

10. Security Controls

- **Multi-Factor Authentication**
- **Encryption**
- **Least Privilege**

- Logging
 - Data Loss Prevention
-

11. Processors & Vendor Management

Vendors must sign DPAs, undergo due diligence, and be audited regularly.

12. Cross-Border Transfers

Standard Contractual Clauses or adequacy decisions will be used for data transfers outside the EU.

13. DPIA / LIA Requirements

DPIAs and LIAs will be conducted as required and approved through internal workflow processes.

14. Incident & Breach Notification

- 1. Detection**
 - 2. Triage**
 - 3. Notification within 72 hours to authorities and affected individuals**
-

15. Training & Awareness

All employees receive mandatory data privacy training and periodic refreshers.

16. Contact Points

- Data Protection Officer (DPO): [Email]**
 - Privacy Contact Mailbox: [Contact Mailbox]**
-

17. Policy Versioning

This policy will be reviewed annually and updated as laws or internal requirements change.

18. Appendix

18.1 Mini-Scenarios

- DSAR request handling
- Vendor onboarding
- Retention deletion run
- Suspected breach escalation

18.2 DSAR Email Template Outline

- Subject
- Request details
- Contact information

18.3 Manager Checklist

- Ensure team compliance
- Report incidents
- Conduct periodic data audits

18.4 FAQ

- 1. What is personal data?**
 - 2. How do I request my data?**
 - 3. What if my data is incorrect?**
 - 4. How long is data retained?**
 - 5. How do I report a breach?**
 - 6. Can I withdraw consent?**
 - 7. How often is this policy reviewed?**
 - 8. Who is the DPO?**
 - 9. What security controls are used?**
- 10. Are vendors compliant?**
- 11. What is a DPIA?**

12. How do I report a privacy concern?

This policy ensures NMT meets its obligations under data protection laws while fostering a culture of privacy awareness.