Data Privacy & GDPR Policy
Version: 2025-01
Company: NMT
Effective Date: 07 December 2025
Review Date: 07 December 2025

---

1. Purpose & Scope

This Data Privacy & GDPR Policy outlines NMT's commitment to safeguarding personal data in accordance with global data protection laws, including the General Data Protection Regulation (GDPR). The policy defines the standards, responsibilities, and operational requirements necessary to ensure lawful, fair, and transparent processing of personal data across all regions where NMT operates.

This policy applies to:

- All employees, contractors, consultants, and third-party processors
- Candidates and applicants participating in recruitment processes
- Customers, clients, and external stakeholders
- All global operations, including EU-based data subjects and systems handling EU personal data

NMT is committed to embedding data privacy into business operations and ensuring continual compliance through responsible data handling and strong governance.

---

2. Key Principles

NMT adheres to the following data protection principles, which form the foundation of all personal data processing activities:

1. **Lawfulness, Fairness, and Transparency** – Data must be processed legally, ethically, and openly.
2. **Purpose Limitation** – Data is collected only for specific, legitimate, and stated purposes.
3. **Data Minimization** – Only the minimum data necessary to achieve the intended purpose is collected and processed.
4. **Accuracy** – Personal data must be kept accurate, complete, and up to date, with prompt correction of inaccuracies.

5. **Storage Limitation** – Data must not be retained longer than necessary for business or legal purposes.
6. **Integrity and Confidentiality** – Appropriate security controls must be applied to prevent unauthorized access, alteration, or loss.
7. **Accountability** – NMT must be able to demonstrate compliance with all data protection obligations.

---

3. Roles & Responsibilities

To ensure effective data governance, the following roles carry defined responsibilities:

- **Data Controller:** Determines the purposes and means of processing personal data.
- **Data Processor:** Processes data on behalf of the Data Controller, complying with contractual and legal requirements.
- **Data Protection Officer (DPO):** Oversees compliance, conducts assessments, manages inquiries, and advises on GDPR obligations.
- **Human Resources (HR):** Ensures proper handling of employee and candidate data throughout the employment lifecycle.
- **Information Technology (IT):** Implements technical controls for secure data storage, transmission, access, and lifecycle management.
- **Managers:** Ensure team-level compliance, support audits, identify risks, and report incidents.
- **Employees:** Adhere to this policy, complete required training, and protect personal and confidential data encountered during their roles.

---

4. Lawful Bases for Processing

Personal data may only be processed when justified by one of the lawful bases under GDPR. NMT relies on:

1. **Contract** – Processing necessary for contractual performance or to enter into a contract.
2. **Legal Obligation** – Required by law or regulatory frameworks.
3. **Vital Interests** – Necessary to protect life or prevent serious harm.
4. **Public Interest** – Processing necessary for public interest tasks where applicable.

5. **Legitimate Interests** – Conducting activities aligned with organizational needs while ensuring individual rights are not overridden.
6. **Consent** – Freely given, informed, and explicit consent where required.

Examples:

- Payroll processing (Contract)
- Tax record retention (Legal Obligation)
- Sending promotional communications (Consent)

---

5. Data Subject Rights

Under GDPR, data subjects are entitled to exercise the following rights:

1. **Right of Access** – Request a copy of personal data held by NMT.
2. **Right to Rectification** – Request correction of inaccurate or incomplete data.
3. **Right to Erasure** – Request deletion of personal data under specific conditions.
4. **Right to Restriction** – Request limited processing of personal data.
5. **Right to Data Portability** – Request transfer of personal data to another controller.
6. **Right to Object** – Object to processing based on legitimate interests or direct marketing.

Handling Timelines:

- Acknowledge requests within **5 business days**
- Provide full response within **30 days**, extendable where permitted by law

---

6. DSAR / Request Handling Process

Process Steps:

1. **Intake** – Receive and log the request via designated channels.
2. **Verification** – Confirm identity to ensure secure response.
3. **Response** – Retrieve, validate, and provide the requested data or outcome.

Service-Level Expectations:

- Acknowledgement issued within **5 days**
- Request fulfilled within **30 days**, unless complexity warrants lawful extension

---

7. Data Classification & Handling Rules

NMT classifies data to ensure that appropriate safeguards match the sensitivity level:

- **Personally Identifiable Information (PII):** Data that identifies an individual (e.g., name, ID numbers).
- **Special Categories:** Sensitive data such as health information, biometric data, racial or ethnic origin.
- **Confidential Data:** Business-sensitive information requiring restricted access.

Handling Rules:

- Encrypt PII during storage and transmission.
- Apply enhanced security controls for special categories of data.
- Restrict access to confidential data strictly on a need-to-know basis.

---

8. Data Collection & Use

NMT collects and processes personal data for legitimate business functions, including:

- Recruitment and onboarding
- Payroll administration and benefits management
- Performance evaluation and employee lifecycle management
- Security monitoring, regulatory reporting, and compliance initiatives

Data is used strictly in alignment with stated purposes and legal bases.

---

9. Retention & Deletion

9.1 Retention Schedule

Data Category **Retention Period**

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 following IT-approved procedures
- Physical shredding of documents containing personal or sensitive information

Retention periods may be adjusted based on updates to legal requirements or operational needs.

---

10. Security Controls

The following security measures must be applied to protect personal data:

- Multi-Factor Authentication (MFA) for system access
- Encryption at rest and in transit
- Least Privilege access model
- Logging and audit trails for sensitive systems
- Data Loss Prevention (DLP) tools to prevent unauthorized disclosure

IT must periodically review and update controls to address emerging threats.

---

11. Processors & Vendor Management

NMT ensures that third-party processors maintain the same level of data protection by requiring:

- Signed Data Processing Agreements (DPAs)
- Completion of due diligence assessments
- Periodic audits, monitoring, and compliance verification

Vendors must be capable of meeting GDPR and internal security obligations.

---

12. Cross-Border Transfers

For international data transfers outside the EU, NMT employs legally valid mechanisms such as:

- Standard Contractual Clauses (SCCs)
- Adequacy decisions issued by the European Commission
- Additional safeguards as required by law

Cross-border transfers must be documented and approved by the DPO.

---

13. DPIA / LIA Requirements

Data Protection Impact Assessments (DPIAs) and Legitimate Interest Assessments (LIAs) are mandatory for high-risk processing activities. These assessments must:

- Identify risks to data subjects
- Outline mitigation strategies
- Be reviewed and approved through NMT's internal governance workflow

---

14. Incident & Breach Notification

Process:

1. **Detection** – Identify unusual activity or potential breach indicators.
2. **Triage** – Assess severity, scope, and affected data types.
3. **Notification** – Notify relevant authorities and affected individuals within **72 hours**, where legally required.

Employees must report suspected incidents immediately.

---

15. Training & Awareness

All employees must complete mandatory data privacy training during onboarding and participate in scheduled refresher courses. Awareness initiatives reinforce best practices, emerging risks, and evolving regulatory requirements.

---

16. Contact Points

- **Data Protection Officer (DPO):** privacy@nmt.com
- **Privacy Contact Mailbox:** dataprotection@nmt.com

These contact points handle queries, concerns, and escalations related to data privacy.

---

17. Policy Versioning

This policy is reviewed annually to ensure alignment with regulatory developments, internal controls, and operational changes. Updates will be documented, approved, and communicated to all employees.

---

18. Appendix

18.1 Mini-Scenarios

- **DSAR Request Handling:** Employee submits access request requiring identity verification and formal response.
- **Vendor Onboarding:** Vendor must undergo due diligence and sign a DPA before processing personal data.
- **Retention Deletion Run:** Scheduled deletion of expired employee records.
- **Suspected Breach Escalation:** Employee reports suspicious system activity triggering breach triage.

18.2 DSAR Email Template Outline

- Subject Line
- Details of the Request
- Required Verification Information
- Expected Response Timelines

18.3 Manager Checklist

- Ensure all team members follow data handling protocols
- Report incidents immediately to DPO or IT Security
- Conduct periodic data audits and ensure corrective actions

This policy ensures that NMT meets its global data protection obligations while promoting a culture of privacy, security, and accountability across the organization.