PLAT4MATION

# Technical and Organisational Measures (TOM)

## For Information Security

7/10/23

# Index

# 1 Organization and Data protection at Plat4mation

In its Information Security and Quality Policy Framework, Plat4mation has set itself the goal, among other things, to provide its customers with the products and services to be delivered at the highest possible level of information security in compliance with the law. This framework enables transparent, sustainable, process-based, and risk-oriented management of the group in the context of industry standards compliance using a Management System (4MMS).

In this context, Plat4mation has established a distinctive security organization to ensure comprehensive protection of its own corporate information and data as well as protection of the data of its customers and clients. The functions of Information Security Officer (ISO), Data Protection Officer (DPO) and Quality Officer (QO) with group-wide responsibility and direct authority in these areas of activity have been established within the staff department "Risk & Compliance", which is directly assigned to the CTO. A comprehensive set of internal guidelines and regulations has been established, which is binding for all employees and defines secure and data protection-compliant handling of information and data.

Employees are continuously informed and trained in data protection. In addition, all employees are contractually bound to data secrecy and confidentiality. External parties who may encounter personal data in the course of their work for Plat4mation are obligated to maintain secrecy and confidentiality as defined in their contracts.

All affiliated companies of the 4Mation Holding BV group of companies within the EU or the EEA have concluded an Intercompany Agreement on Data Protection as a binding written legal instrument pursuant to Art 28 GDPR in order to ensure a uniformly high standard of data protection and data security across the entire group and to clearly regulate the rights and obligations for any commissioned data processing.

Any subcontractors entrusted with further processing (as “other processors”) are only used after approval by the Client as the “controller” and after conclusion of a Data Processing Agreement (DPA) in accordance with Art 28 GDPR, with which they are fully bound by all data protection obligations to which Plat4mation itself is subject.

The organizational measures are supported by Plat4mation’s current, high technical security standards, which are periodically reviewed and confirmed for adequacy and effectiveness in the course of ongoing internal audits and annually by independent, external certification bodies as part of the ISO 9001 and ISO 27001 monitoring and re-certification audits.

# 2 Confidentiality

## 2.1 Physical access control

*Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.*

| Technical Measures | Organizational Measures |
|---|---|
| Alarm system | Gatekeeper / receptionist |
| Automatic access control system | Visitor protocol |
| RFID access system | Employee badges |
| Manual locking system | Care in selection of cleaning services |
| Video surveillance of entrances | Visitor accompanied by employees |
| | Information Security policy |
| | Work instruction access control |

## 2.2 Logical access control

*Measures suitable for preventing data processing systems from being used by unauthorized persons.*

| Technical Measures | Organization Measures |
|---|---|
| Login with username + strong password | User permission management |
| Anti-Virus Software Servers | Creating user profiles |
| Anti-Virus Software Clients | Information Security Policy |
| Firewall | Central password management & SSO |
| Intrusion Detection Systems | Work instruction IT user regulations |
| Use of VPN for remote access | Work instruction operational security |
| Encryption of notebooks / tablet | Work instruction access control |
| Automatic desktop lock | Mobile Device Policy |
| Two-factor authentication | |

## 2.3 Authorisation control

*Measures to ensure that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, modified, or removed without authorization during processing, use and after storage.*

| Technical Measures | Organisational Measures |
|---|---|
| Logging of accesses to applications | Use of authorization concepts |
| Certified SSL encryption | Management of user rights by administrators |
| | Information Security Policy |
| | Minimal access policy |
| | Communication plan information security |

## 2.4 Separation control

*Measures that ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of the data.*

| Technical Measures | Organisational Measures |
|---|---|
| Separation of productive and test environment | Control via authorization concept |
| VLAN segmentation | Information Security Policy |
| Staging dev, test, and production environment | Intercompany Agreement on Data Protection |
| | Security Development policy |

## 2.5 Pseudonymization

*The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.*

| Technical Measures | Organisational Measures |
|---|---|
| N/A | Information Security Policy |
| | Intercompany Agreement on Data Protection |
| | Cryptography policy |

# 3 Integrity

## 3.1 Transfer Control

*Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and establish to which entities personal data are intended to be transmitted by data transmission equipment.*

| **Technical Measures** | **Organisational Measures** |
|---|---|
| Use of VPN | Survey of regular data processes |
| Logging of accesses and retrievals | Information Security Policy |
| Transfer via encrypted connections (TLS) | Minimal Access policy |
| Use of signature procedures | |

## 3.2 Input Control

*Measures that ensure that it is possible to check and establish retrospectively whether and by whom personal data has been entered into, modified or removed from data processing systems. Input control is achieved through logging, which can take place at various levels (e.g., operating system, network, firewall, database, application).*

| **Technical Measures** | **Organisational Measures** |
|---|---|
| Technical logging of the entry, modification, and deletion of data | Traceability of data entry, modification, and deletion through individual users |
| | Assignment of rights to enter, change and delete data based on an authorization concept |
| | Information Security Policy |
| | Acceptable use Policy |

# 4 Availability and Resilience

## 4.1 Availability Control

*Measures to ensure that personal data is protected against accidental destruction or loss (UPS, air conditioning, fire protection, data backups, secure storage of data media, virus protection, raid systems, disk mirroring, etc.).*

| **Technical Measures** | **Organisational Measures** |
|---|---|
| Fire and smoke detection systems | Backup concept and policy |
| UPS system | Existence of an emergency/continuity plan |
| Video surveillance | Storage of backup media in a secure location |
| Locked server/network location | Information Security Policy |
| | Regular testing of continuity plan |

## 4.2 Recoverability Control

*Measures capable of rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.*

| **Technical Measures** | **Organisational Measures** |
|---|---|
| Backup monitoring and reporting | Recovery concept and policy |
| Restorability from automation tools | Control of the backup process |
| Backup concept according to criticality | Regular testing of data recovery and logging of results |
| | Information Security Policy |
| | Storage of backup media in a secure location |
| | Existence of an emergency plan |

# 5 Procedures for regular Review, Assessment and Evaluation

## 5.1 Data Protection Management

| **Technical Measures** | **Organisational Measures** |
|---|---|
| Central documentation of all data protection regulations with access for employees | Internal data protection officer appointed: Group Data Protection Officer. |
| Data protection checkpoints consistently implemented in tool-supported risk assessment | Staff trained and contractually bound to confidentiality/data secrecy |
| A review of the effectiveness of the TOMs is carried out annually and TOMs are updated | Internal Information Security Officer appointed: Group Information Security Officer, CISO. |
| Security certification according to ISO 27001 | Data protection aspects established as part of corporate risk management |
|  | Regular continuous awareness trainings |
|  | ISO 27001 certification of key parts of the company including annual monitoring audits |

## 5.2 Incident Response Management

*Support for security breach response and data breach process*

| **Technical Measures** | **Organisational Measures** |
|---|---|
| Use of firewall and regular updating | Information Security Policy |
| Use of spam filter and regular updating | Data breach procedure |
| Use of virus scanner and regular updating | Security incident policy |
| IDS / IPS In Firewall | Involvement of DPO and (C)ISO in security incidents and data breaches |
|  | Documented process for detecting and reporting security incidents / data breaches (also with regard to reporting obligation to supervisory authority) |
|  | Documentation of security incidents and data breaches via ticket system |

## 5.3 Security by design

*Measures pursuant to Art 25 GDPR that comply with the principles of data protection by design and by default*

| Technical Measures | Organisational Measures |
|---|---|
| Use of data protection-friendly default settings in standard and individual software | Information security policy framework includes ‘security by design’ principles. |
| No more personal data is collected than is necessary for the respective purpose | OWASP Secure Development Security Checks are performed |
| | Perimeter analysis / Pentest for web applications |

## 5.4 Outsourcing / Vendor management

*Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.*

| Technical Measures | Organisational Measures |
|---|---|
| Monitoring of remote access by external parties, e.g. in the context of their activities | Prior review of the security measures taken by the contractor and their documentation |
| Separate VDI available for contractors to access Plat4mation systems | Selection of the contractor under due diligence aspects (especially regarding data protection and data security) |
| | Conclusion of the necessary data processing agreement on commissioned processing or EU standard contractual clauses |
| | Obligation of the contractor's employees to maintain data secrecy based on contracts/NDA. |

# 6 Certification

Both the Quality Management System according to ISO 9001 and the Information Security Management System according to ISO 27001 of essential parts of Plat4mation are certified by an independent third party auditor.

| Measure | GDPR Compliant implemented | Comments |
|---|---|---|
| **Physical Access Control** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Logical Access Control** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Authorization Control** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Separation Control** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Pseudonymization** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Transfer Control** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Input Control** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Availability Control** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Recoverability Control** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Data Protection Management** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Incident Response Management** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Privacy by Design and by Default** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Outsourcing** | ☑ | ISO 27001 Certified, ISO9001 (planned) |
| **Organization** | ☑ | ISO 27001 Certified, ISO9001 (planned) |

TÜV NEDERLAND
ISO 27001