# IT Code of Conduct - The Coding Company B.V.

Introduction

This document describes the code of conduct for the use of IT systems within The Coding Company BV, in accordance with the General Data Protection Regulation (GDPR) and international standards such as ISO27001, ISO27002, ISO 27701:2019, ISO90001 and NEN 7510-1 + A1 + 2.

Our organisation has implemented both technical and organisational measures to safeguard the privacy and integrity of personal data. This code of conduct formalises the responsibilities and obligations of employees and other stakeholders with respect to data protection and IT security.

## Objectives and Scope

This code of conduct applies to all employees, external contractors, and other users of The Coding Company BV's IT systems. The objectives are:

* To ensure a high level of data protection as required by the GDPR (European Union, 2016)
* To protect the confidentiality, integrity, and availability of data (International Organization for Standardization, 2019)
* To minimise risks of data breaches and cyber attacks (Schouten, 2022)

Foundations for Data Protection According to the GDPR, personal data must:

* Be processed lawfully, fairly, and transparently (Art. 5(1) GDPR) (European Union, 2016)
* Be collected and used for specific, explicit, and justified purposes (Art. 5(1)(b) GDPR) (European Union, 2016)
* Be limited to what is necessary for the purposes for which they are processed (Art. 5(1)(c) GDPR) (European Union, 2016)
* Be accurate and updated when necessary (Art. 5(1)(d) GDPR) (European Union, 2016)
* Not be stored longer than necessary (Art. 5(1)(e) GDPR) (European Union, 2016)
* Be processed in a manner that guarantees its security (Art. 5(1)(f) GDPR) (European Union, 2016)

## Organisational Measures

To ensure GDPR compliance, The Coding Company BV utilises the following measures:

* ISO27001 & ISO27701 Certification: This ensures a robust information security policy and privacy management (International Organization for Standardization, 2019)
* Separated Environments: Test, Development, Staging, and Production environments are strictly separated, minimising the impact of data leaks (International Organization for Standardization, 2019)
* Role-Based Access Control (RBAC): System and data access is limited based on job roles and the "need-to-know" principle (Schouten, 2022)
* Confidentiality Obligation: All employees and contractors sign a confidentiality statement to ensure the confidentiality of company data (Schouten, 2022)

## Technical Measures

To comply with GDPR security requirements, the following measures have been implemented:

### Data Encryption:

Files and databases are encrypted with strong encryption standards (Schouten, 2022)

* Encryption is required for sensitive data such as medical and financial information (Art. 32 GDPR) (European Union, 2016)

### Network Security:

* Firewalls, intrusion detection systems (IDS), and VPNs protect the infrastructure (International Organization for Standardization, 2019)
* Network traffic logging and monitoring are actively performed (International Organization for Standardization, 2019)

### Backups and Incident Response:

Regular backups are performed and tested for recoverability (Schouten, 2022). An incident response plan is available and aligned with GDPR (Art. 33 & 34) (European Union, 2016)

## 

## Employee Conduct Rules

Each user of The Coding Company BV's IT systems is responsible for complying with the following conduct rules:

### Strong Authentication:

Multi-Factor Authentication (MFA) is mandatory for all accounts with access to sensitive data (International Organization for Standardization, 2019)

### Email and Phishing Prevention:

Employees must not open suspicious emails or click links without verification (Schouten, 2022). MailThriller is used to analyse and safely present suspicious mail (Schouten, 2022)

### Use of Personal Data:

No copying or storing of personal data on non-approved devices (Schouten, 2022)

### Data Breach Reporting:

Any suspected data breach must be immediately reported to the IT department, in accordance with the data breach notification requirement (Art. 33 GDPR) (European Union, 2016)

### External Storage Media Use:

Use of USB sticks and external drives for sensitive data is prohibited without encryption and IT management approval (International Organization for Standardization, 2019)

### Remote Working Guidelines Company Device Usage:

Use only devices provided by The Coding Company BV (Schouten, 2022)

### Network Security:

Use a secure internet connection and avoid public Wi-Fi (IDEA Consult, 2020)

* **VPN Usage:** Use a secure VPN connection (IDEA Consult, 2020)
* **Data Storage:** No storage on personal devices, only via approved cloud solutions (Schouten, 2022)
* **Conversation Privacy:** Conduct confidential conversations in a closed room (IDEA Consult, 2020)

## 

## Enforcement and Sanctions

Violation of this code of conduct may lead to disciplinary measures, including but not limited to:

* Warnings and mandatory security training (Schouten, 2022)
* Revocation of IT system access rights (Schouten, 2022)
* Legal action for serious violations such as intentional data breaches (European Union, 2016)

### References:

European Union (2016) Verordening (EU) 2016/679 (AVG). Available at:<https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016R0679> (Accessed: 15 April 2023).

European Commission (2019) Gegevensbeschermingsregels als basis voor vertrouwen in de EU. Available at:<https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52019DC0374> (Accessed: 15 April 2023).

International Organization for Standardization (2019) ISO/IEC 27001:2019 - Information Security Management Systems (ISMS). Geneva: ISO.

Schouten, G.J. (2022) De impact op thuiswerken en Work Life Balance. Open Universiteit.

IDEA Consult (2020) Telewerk en beveiligingsmaatregelen in Europa.