IT Code of Conduct

Inleiding

Dit document beschrijft de gedragscode voor het gebruik van IT-systemen binnen The Coding Company BV, in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) en internationale normen zoals ISO27001, ISO27002, ISO 27701:2019, ISO90001 en NEN 7510-1 + A1 + 2.

Onze organisatie heeft zowel technische als organisatorische maatregelen getroffen om de privacy en integriteit van persoonsgegevens te waarborgen. Deze gedragscode formaliseert de verantwoordelijkheden en verplichtingen van medewerkers en andere belanghebbenden met betrekking tot gegevensbescherming en IT-beveiliging.

---

1. Doelstelling en Toepassingsgebied

Deze gedragscode is van toepassing op alle medewerkers, externe contractanten en andere gebruikers van de IT-systemen van The Coding Company BV. De doelstellingen zijn:

- Een hoog niveau van gegevensbescherming te waarborgen, zoals vereist door de AVG [1].
- De vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te beschermen [2].
- De risico's op datalekken en cyberaanvallen te minimaliseren [3].

---

2. Grondslagen voor Gegevensbescherming

Volgens de AVG moeten persoonsgegevens:

1. Rechtmatig, behoorlijk en transparant worden verwerkt (Art. 5(1) AVG) [1].
2. Voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en gebruikt (Art. 5(1)(b) AVG) [1].
3. Beperkt blijven tot wat noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt (Art. 5(1)(c) AVG) [1].
4. Juist zijn en zo nodig worden geactualiseerd (Art. 5(1)(d) AVG) [1].
5. Niet langer worden bewaard dan nodig is (Art. 5(1)(e) AVG) [1].

6. Op een manier worden verwerkt die de beveiliging ervan garandeert (Art. 5(1)(f) AVG) [1].

---

3. Organisatorische Maatregelen

Om de naleving van de AVG te waarborgen, hanteert The Coding Company BV de volgende maatregelen:

- **ISO27001 & ISO27701-certificering**: Dit waarborgt een robuust informatiebeveiligingsbeleid en privacybeheer [2].
- **Gescheiden Omgevingen**: Test-, Development-, Staging- en Productieomgevingen zijn strikt gescheiden, wat de impact van gegevenslekken minimaliseert [2].
- **Rolgebaseerde Toegangscontrole (RBAC)**: Toegang tot systemen en gegevens is beperkt op basis van functierollen en het "need-to-know"-principe [3].
- **Geheimhoudingsplicht**: Alle medewerkers en contractanten tekenen een geheimhoudingsverklaring om de vertrouwelijkheid van bedrijfsgegevens te waarborgen [3].

---

4. Technische Maatregelen

Om te voldoen aan de beveiligingsvereisten van de AVG, zijn de volgende maatregelen geïmplementeerd:

- **Encryptie van Gegevens**:
    - Bestanden en databases worden versleuteld met sterke encryptiestandaarden [3].
    - Versleuteling is vereist voor gevoelige gegevens zoals medische en financiële gegevens (Art. 32 AVG) [1].
- **Netwerkbeveiliging**:
    - Firewalls, intrusion detection systems (IDS) en VPNs beschermen de infrastructuur [2].
    - Logging en monitoring van netwerkverkeer worden actief uitgevoerd [2].
- **Back-ups en Incident Response**:
    - Regelmatige back-ups worden uitgevoerd en getest op herstelbaarheid [3].
    - Een incidentresponsplan is beschikbaar en in lijn met de AVG (Art. 33 & 34) [1].

---

5. Gedragsregels voor Werknemers

Iedere gebruiker van de IT-systemen van The Coding Company BV is verantwoordelijk voor het naleven van de volgende gedragsregels:

1. **Sterke authenticatie gebruiken**:
    - Multi-Factor Authenticatie (MFA) is verplicht voor alle accounts met toegang tot gevoelige gegevens [2].
2. **E-mail en Phishing Preventie**:
    - Medewerkers mogen geen verdachte e-mails openen of op links klikken zonder verificatie [3]. Tevens wordt gebruikgemaakt van MailThriller die verdachte mail analyseert en veilig presenteert.
3. **Gebruik van Persoonsgegevens**:
    - Geen persoonsgegevens kopiëren of opslaan op niet-goedgekeurde apparaten [3].
4. **Datalekken melden**:
    - Elk vermoeden van een datalek moet onmiddellijk worden gemeld aan de IT-afdeling, in overeenstemming met de meldplicht datalekken (Art. 33 AVG) [1].
5. **Gebruik van Externe Opslagmedia**:
    - Het gebruik van USB-sticks en externe schijven voor gevoelige gegevens is verboden zonder encryptie en toestemming van IT-beheer [2].

---

6. Richtlijnen voor Thuiswerken

- **Gebruik van Bedrijfsapparatuur**: Gebruik uitsluitend door The Coding Company BV verstrekte apparaten [4].
- **Netwerkbeveiliging**: Gebruik een beveiligde internetverbinding en vermijd openbare Wi-Fi [5].
- **VPN-gebruik**: Maak gebruik van een beveiligde VPN-verbinding [5].
- **Opslag van Gegevens**: Geen opslag op persoonlijke apparaten, enkel via goedgekeurde cloudoplossingen [4].
- **Privacy van Gesprekken**: Voer vertrouwelijke gesprekken in een afgesloten ruimte [5].

---

7. Handhaving en Sancties

Schending van deze gedragscode kan leiden tot disciplinaire maatregelen, inclusief maar niet beperkt tot:

- Waarschuwingen en verplichte beveiligingstrainingen [3].
- Intrekking van toegangsrechten tot IT-systemen [3].
- Juridische stappen bij ernstige overtredingen zoals opzettelijke datalekken [1].

Bibliografie

1. Europese Unie (2016). *Verordening (EU) 2016/679 (AVG)*. Beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32016R0679.
2. Europese Commissie (2019). *Gegevensbeschermingsregels als basis voor vertrouwen in de EU*. Beschikbaar op: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52019DC0374.
3. ISO (2019). *ISO/IEC 27001:2019 - Information Security Management Systems (ISMS)*. Genève: International Organization for Standardization.
4. Schouten, G.J. (2022). *De impact op thuiswerken en Work Life Balance*. Open Universiteit.
5. IDEA Consult. (2020). *Telewerk en beveiligingsmaatregelen in Europa*.