Data Breach Protocol - Dailyflex Personeelsdiensten B.V.

Last revised*: 01-01-2025*

1. Purpose

The purpose of this protocol is the timely **detection**, **investigation**, **registration**, **handling**, and – if necessary – **reporting** of (suspected) data breaches, in accordance with the **General Data Protection Regulation (GDPR)**.

This protocol safeguards the privacy of data subjects and ensures legal accountability for **Dailyflex Personeelsdiensten B.V.**

2. What is a data breach?

A **data breach** is a security incident in which personal data is lost or unintentionally becomes accessible to unauthorized persons. Examples include:

- Loss of a USB stick or laptop containing personal data
- Access to personal data by an unauthorized person
- Personal data sent to the wrong recipient
- Hacking, phishing, or ransomware attack
- Data exfiltration
- Security vulnerability in software

3. Reporting a data breach

Any employee or processor who detects a (potential) data breach must **immediately report** this to:

Primary contact
Henriëtte van Santen
Functionaris Gegevensbescherming (FG)
T 0174 - 28 72 73
M 06 - 83 02 15 26
E henriette@dailyflex.nl

Secondary contact
Ronald Saarloos
Algemeen Directeur
T 0174 - 28 72 73
M 06 - 83 02 15 26
E ronald@dailyflex.nl

Include in your report (if known):

- Date and time of discovery
- Brief description of the incident
- Systems or data involved
- Name of the reporter
- Contact details of the reporter

4. Assessment of the report
The DPO or a designated responsible person will carry out the following:
Verification
Determine whether a data breach has actually occurred

Risk analysis, in accordance with the Dutch Data Protection Authority (AP) guidelines:

- Type of data leaked (e.g., special categories, financial data)
- Number of data subjects affected
- Consequences for data subjects
- Protection level (e.g., encrypted?)

Documentation
Register the incident in the internal data breach log, regardless of reporting obligations

5. Notification to the Dutch Data Protection Authority (AP)
If there is a risk to the rights and freedoms of data subjects, a notification must be made within **72 hours** via: autoriteitpersoonsgegevens.nl > Melden datalek

The report includes:

- Description of the incident
- Type and scope of data leaked
- Number of affected data subjects
- Measures taken or planned
- Contact person for the AP
- Assessment of consequences

Failure to report or late reporting may result in fines.

6. Informing data subjects
If there is a **high risk** to the rights and freedoms of data subjects, they must be informed directly.
Examples:

- Leaked BSN (Citizen Service Number) or medical data
- Large number of affected persons (10 or more)
- Easily misused data
- Other risk factors relevant to Dailyflex

Communication methods may include:

- Email
- Letter
- Telephone

The notification must contain:

- Clear description of the breach
- Possible consequences
- Contact details at Dailyflex
- Measures already taken
- Advice to the data subject (e.g., change password)

7. Internal registration

All data breaches are recorded, including those not subject to mandatory reporting. The register contains:

- Date and time of incident and discovery
- Description of the incident
- Involved systems/personnel
- Type of data
- Number of data subjects affected
- Risk assessment
- Measures taken
- Reporting status (to AP and/or data subjects)
- Evaluation (lessons learned)

Retention period: 2 years

8. Prevention and training

Training & awareness (annually):

- GDPR and privacy principles
- Recognizing data breaches
- Reporting procedures
- Practical importance of data protection

Technical & organizational measures:

- Access control (roles and rights)
- Strong passwords and MFA policy
- Encryption (at rest and in transit)
- Up-to-date firewall and antivirus
- Regular backups and recovery procedures
- Annual penetration testing
- Patch management and updates

Annual evaluation:

- Effectiveness of measures
- Data breach analysis
- Procedure testing
- Updates in legislation and technology

9. Processor agreements

If Dailyflex acts as a processor, all data processing agreements are periodically evaluated against this protocol. Any deviations are documented explicitly.