Privacybeleid FinFixers - NL

1. Inleiding

1.1 Achtergrond

FinFixers werkt met persoonsgegevens van kandidaten, opdrachtgevers en medewerkers. Om te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) zijn er maatregelen genomen om data te beschermen. Dit rapport geeft inzicht in de genomen maatregelen. Hiermee laten we zien hoe FinFixers verantwoording aflegt over de naleving van de AVG.

---

2. Overzicht van gegevensverwerkingen

2.1 Inventarisatie

Er is een **register van verwerkingsactiviteiten** opgesteld waarin de volgende categorieën persoonsgegevens zijn opgenomen:

1. **Kandidaten**
    - Naam, adres, woonplaats, contactgegevens (telefoon/e-mail), geboortedatum, opleidingsniveau, werkervaring, CV, referenties.
    - Grondslag: toestemming (voor bewaren CV) en uitvoering van (voorbereiding op) een overeenkomst.
2. **Opdrachtgevers (contactpersonen)**
    - Naam, e-mailadres, telefoonnummer, functie, bedrijf.
    - Grondslag: uitvoering overeenkomst en gerechtvaardigd belang (zakelijke communicatie).
3. **Medewerkers FinFixers**
    - Persoonsgegevens nodig voor salarisadministratie en personeelsbeheer (naam, BSN, bankrekeningnummer, adres, contract).
    - Grondslag: wettelijke verplichting (loonbelasting), uitvoering arbeidsovereenkomst.
4. **Websitegebruikers**
    - IP-adres en cookiegegevens
    - Grondslag: toestemming (voor niet-essentiële cookies) en gerechtvaardigd belang (analyses en basisfunctionaliteit).

2.2 Bewaartermijnen

- **Kandidaten**: 1 jaar na laatste contactmoment, tenzij kandidaat expliciete toestemming heeft gegeven voor langer bewaren.
- **Opdrachtgevers**: tot 7 jaar na afloop van de overeenkomst (i.v.m. fiscale en wettelijke verplichtingen).

- **Medewerkers**: 7 jaar na einde dienstverband voor fiscale zaken; overige gegevens worden uiterlijk 2 jaar na uitdiensttreding vernietigd (tenzij wettelijke bewaarplicht geldt).

---

3. Beveiliging

1. **Encryptie & toegangsbeheer**
    - Sterke wachtwoorden en versleutelde opslag voor gevoelige gegevens zijn ingevoerd.
2. **Datalekprotocol**
    - Er is een intern meldproces opgesteld; medewerkers melden mogelijke incidenten direct bij de directie.

Privacy policy FinFixers - EN

1. Introduction

1.1 Background

FinFixers works with personal data of candidates, clients, and employees. To comply with the General Data Protection Regulation (GDPR), measures have been taken to protect data. This report provides insight into these measures. It demonstrates how FinFixers takes responsibility for complying with the GDPR.

---

2. Overview of Data Processing

2.1 Inventory

A register of processing activities has been drawn up, which includes the following categories of personal data:

1. **Candidates**
    - Name, address, place of residence, contact details (phone/email), date of birth, educational level, work experience, CV, references.
    - **Legal basis:** Consent (for storing the CV) and performance of (preparation for) a contract.
2. **Clients (contact persons)**
    - Name, email address, phone number, job title, company.
    - **Legal basis:** Performance of a contract and legitimate interest (business communication).
3. **FinFixers Employees**
    - Personal data required for payroll administration and personnel management (name, citizen service number (BSN), bank account number, address, employment contract).
    - **Legal basis:** Legal obligation (payroll tax) and performance of an employment contract.
4. **Website Users**
    - IP address and cookie data.
    - **Legal basis:** Consent (for non-essential cookies) and legitimate interest (analytics and basic functionality).

2.2 Retention Periods

- **Candidates:** 1 year after the last contact, unless the candidate has given explicit consent for longer storage.
- **Clients:** Up to 7 years after the end of the contract (due to tax and legal obligations).
- **Employees:** 7 years after termination of employment for tax purposes; other data is destroyed no later than 2 years after the end of employment (unless there is a legal obligation to retain it).

---

3. Security

1. **Encryption & Access Management**
    - Strong passwords and encrypted storage for sensitive data have been implemented.
2. **Data Breach Protocol**
    - An internal reporting process has been set up; employees must immediately report any potential incidents to management.
