Data Privacy Policy

V2025.04

1. Introduction

Wonderkind Global B.V., hereafter referred to as **Wonderkind**, is committed to maintaining the highest standards of privacy and data protection. This policy outlines the principles Wonderkind follows to process data transparently, responsibly, and securely in compliance with applicable regulations, including the General Data Protection Regulation (GDPR).

This policy is supplemented by:

- **Appendix 1:** Technical and Organisational Measures.
- **Appendix 2:** Sub-processors.

2. Nature of the Services

- Wonderkind facilitates job promotion by distributing job ads on selected Advertising Platforms.
- Wonderkind does not collect, store, or process candidate data. All applications and candidate interactions occur outside of Wonderkind's scope.
- Users remain responsible for the content and compliance of their job ads, including adherence to platform-specific policies.

3. User Responsibilities

Users must ensure that job postings:

- Comply with all applicable laws, including anti-discrimination regulations.
- Do not contain misleading, deceptive, or unlawful content.
- Acknowledge that Wonderkind does not guarantee ad performance, as results depend on budget, audience targeting, and Advertising Platform algorithms.
- Remain solely responsible for interactions with applicants and must comply with relevant privacy laws (e.g., GDPR, CCPA).
- Adhere to the content policies of the Advertising Platforms:

- Meta Advertising Standards
- Google Ads Policies
- Snapchat Advertising Policies
- TikTok Ad Policies

4. Advertising Platforms & Policy Compliance

- Job ads may be distributed via Meta, Google, Snapchat, and TikTok.
- Each platform enforces its own advertising policies, which users must comply with. Policy violations may result in ad removal or suspension.
- Users agree that Wonderkind has discretion over ad placement and optimization to maximize campaign effectiveness.

5. Scope of Data Processing

Wonderkind processes only limited user data, such as:

- Personal Information: Name, email address, and login credentials for platform access.

Wonderkind does not process candidate data, which remains under the control of the respective Advertising Platform(s) per their privacy policies.

6. Duty to Report

In the event of a security leak and/or data breach, as referred to in Article 33 of the GDPR, Wonderkind will, to the best of its ability, notify the relevant customers and users of the Wonderkind Platform without undue delay. The customer will determine whether to inform its end-users, Data Subjects, and/or relevant regulatory authorities.

This duty to report applies irrespective of the impact of the leak. Wonderkind will endeavor to provide complete, accurate, and timely information, including:

- The (suspected) cause of the breach.

- The (currently known or anticipated) consequences.
- The (proposed) solution.
- The measures already taken.

If required by law or regulation, Wonderkind will cooperate in notifying the relevant authorities and/or Data Subjects.

7. Security

In accordance with Article 32 of the GDPR, Wonderkind will take adequate technical and organisational measures to protect customer and user data against:

- Loss.
- Unauthorised disclosure.
- Deterioration.
- Alteration or unlawful processing.

The details of these measures are outlined in Appendix 1: *Technical and Organisational Measures.*

Wonderkind does not guarantee that security measures will be effective under all circumstances. However, the measures implemented are designed to maintain a reasonable level of protection based on:

- The state of the art.
- The sensitivity of the data.
- The costs associated with the measures.

Customers and users of the Wonderkind Platform are responsible for ensuring that they comply with the agreed security measures before providing personal data to Wonderkind.

8. Sub-processors

Wonderkind engages sub-processors to deliver its services. The details of the current sub-processors are listed in Appendix 2: *Sub-processors.*

The list of sub-processors may change to reflect the evolving needs of the services. Wonderkind will notify customers of updates where appropriate and in compliance with applicable regulations.

9. Rights of Data Subjects

Customers and users of the Wonderkind Platform have the right to:

- Access, correct, or delete their data.
- Restrict or object to data processing.
- Lodge complaints with relevant authorities.

10. Data Retention

Wonderkind retains personal data only as long as necessary to fulfil the purposes outlined in this policy or as legally required. Specifically:

1. **Retention Period**:
    - Personal data is retained for the duration of the User Agreement.
    - Upon the expiry or termination of the User Agreement, Wonderkind reserves the right to retain personal data for up to 90 days to facilitate account closure, resolve disputes, or comply with legal obligations.
2. **Deletion or Anonymisation**:
    - After the 90-day period, personal data will either be securely deleted or anonymized, unless further retention is required by law or in the case of ongoing legal claims or disputes.
3. **User Rights**:
    - Users may request the deletion of their personal data before the 90-day retention period, subject to applicable legal or contractual obligations.

11. Updates

Wonderkind reserves the right to update this policy as needed. Significant changes will be communicated through the platform.

12. Data Classification and Handling

Wonderkind classifies all personal data it processes under a structured classification scheme, as follows:

- Public: Data intended for public disclosure. (Not applicable to personal data)

- Internal: Operational or process information not classified as personal data.

- Confidential: All personal data processed (name, email address, login credentials).

- Restricted: Not applicable, as Wonderkind does not process special category or sensitive data.

Based on this classification, the following handling measures apply to Confidential data (i.e., all personal data):

- Encryption in transit using HTTPS (TLS 1.2+) and at rest using AES-256.

- Passwords hashed using industry-standard algorithms.

- Strict role-based access control and least privilege enforcement.

- Multi-factor authentication for all critical systems.

- Logging and periodic access reviews.

Appendix 1: Technical and Organisational Measures

This appendix outlines the specific measures Wonderkind takes to secure data, ensuring alignment with the **Security** section of the policy:

1. **Quality Management**: Rigorous quality management procedures, including automated and manual testing, are implemented before deploying new features or resolving defects.
2. **Code Inspection**: All newly developed code undergoes a senior developer review, ensuring adherence to secure coding standards before production deployment.
3. **HTTPS Protocol**: All personal data transfers over the internet are encrypted using HTTPS.
4. **Password Storage**: Passwords are stored following industry standards, utilizing robust hashing algorithms.
5. **Penetration Testing**: Periodic penetration tests are conducted by external specialists to assess system security.
6. **Data Backups**: All personal data is backed up daily or incrementally to prevent data loss.
7. **Access Management**: Access to personal data is granted only to authorized employees with a strict need-to-know policy; access is revoked when no longer required.
8. **Data Center Security**: Data is hosted exclusively in ISO 27001-certified data centers with stringent security measures and high availability.
9. **DDoS Mitigation**: Defensive measures are in place to protect against Layer 4 (and lower) DDoS attacks.
10. **Firewall Protection**: Firewalls protect the infrastructure against unauthorised access.

Data Privacy Policy Appendix 2

This appendix outlines Wonderkind's use of sub-processors, aligning with the **Sub-processors** section of the policy:

1. **Microsoft Azure**
    - **Entity Name**: Microsoft Corporation and its sub-processors.
    - **Purpose**: Data hosting and storage.
    - **Data Processing Location**: West Europe (Netherlands).
    - **Additional Information**: Details are available on Microsoft's Service Trust Portal.
2. **Auth0 (Okta Identity Netherlands BV)**
    - **Entity Name**: Okta Identity Netherlands BV.
    - **Purpose**: Identity management and authentication.
    - **Data Processing Location**: EU-2.

Version Control

Document Version: 2025.04 (Official Replacement)

Replaces: v2025.01, v2025.02 and v2025.03

Last Updated: March 27, 2025

Maintained by: privacy@wonderkind.com