

European Data Privacy Transparency Notice for Employee Applicants

Agendia N.V. at Radarweg 60, 1043 NT Amsterdam, The Netherlands, and its subsidiaries including its affiliated company in the United States, Agendia, Inc., (collectively referred to herein as “Agendia”), are committed to adhering to applicable data protection laws. Agendia recognizes and respects the privacy rights of individuals with regard to their Personal Data. Personal Data can be factual (for example, a name, email address, location, or date of birth) or anything related to that person’s actions or behavior. If you are from the European Union (EU), this Data Privacy Transparency Notice will explain Agendia’s legal basis for collecting and using your Personal Data and the specific context in which we collect it.

Personal Data Collected

Most often, the personal data that Agendia collects from employee applicants is collected from them directly. In some cases, we may collect personal data about employee applicants from third parties, for example when we perform background checks. In most circumstances, we will get your permission before we collect personal data about you from a third party. Collected and stored personal data can appear in the form of:

- *Background Checks* – such as such as criminal history, criminal records, driving citations, reference or background checks
- *Browsing Information* – such as cookie information, IP address, website history
- *Contact Information* – such as emergency contact details, home address, personal email, and phone numbers
- *Education & Skills* – such as education & training history, educational degrees, grades, and languages
- *Employment Information* – such as job application details, job title/role, previous work history, record of absence, salary/wage expectation, start date
- *Government Identifiers* – such as driving license number, national identification number, national identity card details, passport number, and social security number
- *Personal Identification* – such as citizenship status, date of birth, disability or specific conditions, full name, gender, marital status, military or veteran status, nationality, racial or ethnic origin, signature and unique identification numbers for HCPs
- *Professional Experience & Affiliations* – such as professional memberships and qualifications/certifications
- *Social* – such as social media accounts and contacts
- *Travel & Expenses* – such as travel booking details and travel history

If we ask you to provide any other personal data not described above, then the personal data we will ask you to provide, and the reasons why we ask you to provide it, will be made clear to you at the point we collect it.

How Personal Data is Used

Agendia uses and discloses the personal data that we collect primarily for the purposes of managing our employment relationship with you, along with other business purposes. Such uses include:

- Determining eligibility for hiring, including the verification of references and qualifications and, where permitted by law, administering of background checks;
- Complying with laws and regulations (e.g., labor and employment laws, health and safety, tax, anti-discrimination laws), under judicial authorization, or to exercise or defend legal rights;

Legal Basis for Processing Personal Data

If you are an employee in the European Economic Area (EEA), our legal basis for collecting and using the personal data described above will depend on the personal data concerned and the context in which we collect it.

However, we will normally collect personal data from you only where we have:

- *Legitimate Interest* – Applies if the processing activity is strictly necessary for a legitimate purpose pursued by Agendia acting as the data controller or a third party when the employee's rights and interests are fully considered and protected. An internal operation like payroll is an example of a legitimate interest.
- *Contracts* – The data processing activity is necessary for the performance of a contract with the employee. An employment agreement would be an example.
- *Legal Requirement* – Agendia could be subject to compliance with laws, obligations, and statutes. For example, a governing body may request wage information.
- *Vital Interests* - In some cases, we may need the personal data to protect your vital interests or those of another person (for example, we may need to share your personal data with third parties in the event of an emergency at work).
- *Consent* – In rare instances, Agendia may ask an employee for their expressed consent to process their data. Consent must be freely given and can be withdrawn at any time. An example would be asking to use an employee's photo on the website.

With Whom Do We Share Your Data?

We take care to allow your personal data to be accessed only by those who really need to in order to perform their tasks and duties, and to third parties who have a legitimate purpose for accessing it.

When acting as a data controller, we may share your personal data with other employees, other Agendia group companies, contractors, consultants, and service providers who require the data to assist Agendia to establish, manage or terminate your employment with Agendia, including parties that provide products or services to us or on our behalf. Data controllers are those who collect the data in question and determine how it will be used.

For example, we engage third parties such as employee benefit plan providers (Cigna), payroll support services (Paylocity), and employee travel management services (Uniglobe). In some cases, these parties may also provide certain IT and data processing services to us so that we can operate our business.

When we share personal data with these parties for specific tasks, referred to as processors, we typically require that they use or disclose that personal data only as instructed by Agendia and in a

manner consistent with this Privacy Notice and applicable laws. We also enter contracts with these parties to make sure they respect the confidentiality of your personal data and have appropriate data security measures in place.

If we go through a corporate sale, merger, reorganization, dissolution or similar event, personal data we gather from you may be transferred in connection with such an event. Any acquirer or successor of Agendia may continue to use the data as described in this notice provided that the acquirer or successor is bound by appropriate agreements or obligations and may only use or disclose your personal data in a manner consistent with the use and disclosure provisions of this notice, or unless you consent otherwise.

We may also disclose your personal data to a third party under the following circumstances:

- if we in good faith believe we are compelled by any applicable law, regulation, legal process, or government authority;
- where necessary to exercise, establish or defend legal rights, including to enforce our agreements and policies;
- to protect Agendia's rights or property;
- in connection with regular reporting activities to other members of the Agendia corporate family;
- to protect Agendia, our other customers, or the public from harm or illegal activities;
- to respond to an emergency which we believe in good faith requires us to disclose data to prevent harm; or
- with your consent, which you have the right to withdraw your consent at any time, such as website cookie tracking.

International Operations and Transfers Out of Your Home Jurisdiction

Your personal data may be collected, used, processed, stored, or disclosed by us and our service providers outside your home jurisdiction, including in the U.S., and in some cases, other countries. These countries may have data protection laws that are different the laws of your country. Agendia only transfers personal data to another country, including within the Agendia corporate family, in accordance with applicable privacy laws, and provided there is adequate protection in place for the data.

How Do We Secure Your Data?

We use appropriate technical and organizational security measures to protect the security of your personal data both online and offline including the implementation of access controls, implementation of firewalls, network intrusion detection and use of anti-virus software. Please note that no system is completely secure.

How Do You Update Your Personal Data?

It is important that the information contained in our records is both accurate and current. We offer various self-help tools that will allow you to update certain of your personal data in our records. If your personal data changes, please use these self-help tools to update that data, where available, or let HR (hr.ets@agendia.com) know of those changes.

How Can You Request Access to Your Personal Data?

Please make this request to our HR department in writing (email is fine, hr.ets@agendia.com). We may ask you for information to verify your identity and evaluate your right to access the personal data requested. You can also ask that we delete personal data that you believe is inaccurate or no longer

relevant in this same way. Of course, we might need to refuse access to, or deletion of, personal information in certain cases, such as when providing access might infringe someone else's privacy rights or impact our legal obligations.

What Other Rights Do You Have Over Your Personal Data?

You have the right to request access of an overview of your personal data, and under certain conditions, rectification and/or erasure of personal data. In addition, you may also have the right of restriction of processing concerning your personal data, the right to object to processing as well as the right to data portability.

For example, if we have collected and processed your personal data with your consent, then you have the right to withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we carried out prior to your withdrawal, nor will it affect processing of your personal data carried out in reliance on other lawful grounds other than consent.

How Long Do We Retain Your Personal Data?

We will keep your personal data for as long as is needed to carry out the purposes we've described above, or as otherwise required by law. Generally, this means we will keep your personal data until the end of your employment application process with us, plus a reasonable period after that where necessary to respond to any employment inquiries, deal with legal, tax, accounting, or administrative matters, or to provide you with ongoing pensions or other benefits.

For employee applicant personnel records, that retention period is 7 years after the applicant's relationship with Agendia has ended.

Where we have no continuing legitimate business need to process your personal data, we will either delete or anonymize it or, if this is not possible (for example, because your personal data has been stored in backup archives), then we will securely store your personal data and isolate it from any further processing until deletion is possible.

Contact Details

You can get in touch with an Agendia data privacy representative at:

- Agendia N.V.
- Address: Radarweg 60, 1043 NT Amsterdam, The Netherlands
- You can contact our Privacy department at privacy@agendia.com and our Data Protection Officer (DPO) at dpo@agendia.com

Employees have the right to lodge a complaint to the Dutch Data Protection Authority with the information below:

- Autoriteit Persoonsgegevens
- PO Box 93374
2509 AJ DEN HAAG
- Telephone number: (+31) - (0)70 - 888 85 00
- Fax: (+31) - (0)70 - 888 85 01
- Visiting address(only by appointment)
Bezuidenhoutseweg 30
2594 AV Den Haag