

DATA PRIVACY STATEMENT

Processing of (personal) data by the entity in charge of the online application process

General information

This data privacy statement, which refers exclusively to data collected as part of the online application process, is to inform you about how your personal data that is collected as part of the online application process is handled at our end.

The controller

The controller under data protection law is:

EXTOLL GmbH

Rheinvorlandstraße 5, 68159 Mannheim, Germany

Phone: +49 (0)621 124 765-00

Commercial register entry number: HRB 711590

Registration Court: Reg. - Gericht Mannheim

Email: general-data-protection-regulation@extoll.com

Personal data collected as part of the application process

Personal data means any information concerning the personal or material circumstances of an identified or identifiable individual. This includes information such as, for example, your name, address, telephone number and date of birth, but also data relating to your specific career etc. by reference to which a specific individual can be identified with reasonable effort. However, information which cannot be (in)directly associated with your real-life identity is not personal data.

Fundamentals and purposes of processing personal data collected from application documents and during the application process

If you apply to us electronically, i.e. via e-mail or using our online form, we will collect and process your personal data for the purpose of executing the application process and preparing contracts.

By submitting an application via our recruitment website, you express your interest in taking up work with us. In this context, you transmit personal data, which we will use and store exclusively for the purpose of your job search / application process.

In particular, the following data is collected during this process:

name (first and last names)

e-mail address

phone number

LinkedIn profile (optional)

channel through which you found us

Furthermore, you can choose to upload expressive documents such as a cover letter, your CV and reference letters. These may contain additional personal data such as date of birth, address etc.

Only authorized HR staff and/or staff involved in the application process have access to your data.

The personal data is stored, as a rule, exclusively for the purpose of filling the vacancy for which you have applied.

Your data will be stored for a period of 180 days after the application process has been concluded. This is usually done to fulfill legal requirements and/or defending ourselves against any claims arising from legal provisions. After this period, we are obligated to delete or anonymize your data. In case of anonymization, the data will only be available to us in the form of so-called metadata, without any direct personal reference, for statistical analysis (for example, share of male and/or female applicants, number of applications per specified period of time etc.).

Furthermore, we reserve the right to store your data for 365 days after the application process has been concluded for the purpose of adding it to our Talent Pool in order to identify any other vacancies that may be of interest to you. This includes, for example, applications for apprenticeships or internships. By accepting the data privacy statement, you consent to any further storage of your data as well as its inclusion in our Talent Pool. For this, we will ask you for your permission.

Should you be offered and accept a position with us during the application process, we will store the personal data collected as part of the application process for at least the duration of your employment.

Disclosure of data to third parties

Data transmitted as part of your application will be transferred using TLS encryption and stored in a database. This database is operated by Personio GmbH, which offers a human resource and applicant management software solution (<https://www.personio.com/legal-notice/>). In this context, Personio is our processor under article 28 of the GDPR. In this case, the processing is based on an agreement for the processing of orders between us as the controller and Personio.

Rights of data subjects

If we as the controller process personal data, you as the data subject have certain rights under Chapter III of the EU General Data Protection Regulation (GDPR), depending on the legal basis and the purpose of the processing, in particular the right of access (article 15 of the GDPR) and the rights to rectification (article 16 of the GDPR), erasure (article 17 of the GDPR), restriction of processing (article 18 of the GDPR), and data portability (article 20 of the GDPR), as well as the right to object (article 21 of the GDPR). If the personal data is processed with your consent, you have the right to withdraw this consent under article 7 III of the GDPR. To assert your rights as a data subject in relation to the data processed during this online application process, please refer to our Data Protection Officer (see item 2).

Concluding provisions

We reserve the right to adjust this data privacy statement at any point in time to ensure that it is in line with the current legal requirements at all times, or in order to accommodate changes in the application process or other processes. In this case, the new data privacy statement applies to any later visit of this recruitment website or any later job application. In addition to this data privacy statement, please view our general data privacy statement.

Processing of (personal) data by the operator of the recruitment website

General information

This recruitment website is operated by Personio SE & Co. KG, which offers a human resource and candidate management software solution (<https://www.personio.com/legal-notice/>). Data transmitted as part of your application will be transferred using TLS encryption and stored in a database. The sole controller of this data within the meaning of article 24 of the GDPR is the enterprise carrying out this online application process. Personio's role is limited to operating the software and this recruitment website and, in this context, being a processor under article 28 of the GDPR. In this case, the processing by Personio is based on an agreement for the processing of orders between the controller and Personio. In addition, Personio SE & Co. KG processes further data, some of which may be personal data, to provide its services, in particular for operating this recruitment website. We will refer to this in more detail below.

The controller

The controller under data protection law is:

Personio SE & Co. KG

Seidlstraße 3

80335 München

Tel.: +49 (89) 1250 1004

Entry in the commercial register

Commercial register entry number: HRA 115934

Registration Court: Amtsgericht München

Data Protection Officer contact: privacy@personio.com

Access logs ("server logs")

Each access to this recruitment website automatically causes general protocol data, so-called server logs, to be collected. As a rule, this data is a pseudonym and thus does not allow for inferences about the identity of an individual. Without this data, it would, in some cases, be technically impossible to deliver or display the contents of the software. In addition, processing this data is absolutely necessary under security aspects, in particular for access, input, transfer, and storage control. Furthermore, this anonymous information can be used

for statistical purposes and for optimizing services and technology. In addition, the log files can be checked and analyzed retrospectively when unlawful use of the software is suspected. The legal basis for this is §25 subsection 2 Sentence 2 TTDSG. Generally, data such as the domain name of the website, the web browser and web-browser version, the operating system, the IP address, as well as the timestamp of the access to the software is collected. The scope of this log process does not exceed the common log scope of any other site on the web. These access logs are stored for a period of up to 7 days. There is no right to object to this.

Error logs

So-called error logs are generated for the purpose of identifying and fixing bugs. This is absolutely necessary to ensure we can react as quickly as possible to possible problems with displaying and implementing content (legitimate interest). As a rule, this data is a pseudonym and thus does not allow for inferences about the identity of an individual. The legal basis for this is §25 subsection 2 Sentence 2 TTDSG. When an error message occurs, general data such as the domain name of the website, the web browser and web-browser version, the operating system, the IP address, as well as the timestamp upon occurrence of the respective error message and/or specification is collected. These error logs are stored for a period of up to 7 days. There is no right to object to this.

Use of cookies

So-called cookies are used on parts of this recruitment website. They are small text files which are stored on the device with which you access this recruitment website. As a general rule, cookies serve the purpose of ensuring secure access to a website ("absolutely necessary"), implementing certain functionalities such as standard-language settings ("functional"), improving the user experience or the performance of the website ("performance"), or placing targeted advertisements ("marketing"). On this recruitment website, we generally use only cookies that are absolutely necessary, functional or performance-related, in particular for implementing certain default settings such as language, for identifying the job advertising channel, or for analyzing the performance of a job advert via which a user accessed this recruitment website. The use of cookies is absolutely necessary for providing our services and thus for the performance of the contract (article 6 (1) b) of the GDPR). Period of storage: up to 1 month or until the end of the browser session Right to object: You can determine via your browser settings whether you allow or object to the use of cookies. Please note that deactivating cookies may result in limited or completely blocked functionalities of this recruitment website.

Rights of data subjects

If Personio SE & Co. KG as the controller processes personal data, you as the data subject have certain rights under Chapter III of the EU General Data Protection Regulation (GDPR), depending on the legal basis and the purpose of the processing, in particular the right of access (article 15 of the GDPR) and the rights to rectification (article 16 of the GDPR), erasure (article 17 of the GDPR), restriction of processing (article 18 of the GDPR), and data portability

(article 20 of the GDPR), as well as the right to object (article 21 of the GDPR). If the personal data is processed with your consent, you have the right to withdraw this consent under article 7 III of the GDPR. To assert your rights as a data subject in relation to the data processed for the purpose of operating this recruitment website, please refer to Personio SE & Co. KG's Data Protection Officer (see item B).

Concluding provisions

Personio reserves the right to adjust this data privacy statement at any point in time to ensure that it is in line with the current legal requirements at all times, or in order to accommodate changes in the services offered, for example when new services are introduced. In this case, the new data privacy statement applies to any later visit of this recruitment website or any later job application.

Introduction

We take the privacy of our website users very seriously and are committed to protecting the information that users provide to us in connection with their use of our website. We are also committed to protecting and using your information in accordance with applicable law.

This Privacy Policy explains our practices regarding the collection, use and disclosure of your information through the use of our digital assets (the "Services") when you access the Services through your devices.

Please read the Privacy Policy carefully and make sure you fully understand our practices with respect to your information before using our Services. If you have read and fully understand this policy and do not agree with our practices, you must stop using our digital assets and services. By using our Services, you agree to the terms of this Privacy Policy. Your continued use of the Services constitutes your acceptance of this Privacy Policy and any changes to it.

This Privacy Policy tells you:

- How we collect data
- What data we collect
- Why we collect this data
- Who we share the data with
- Where the data is stored
- How long the data is retained
- How we protect the data
- How we deal with minors
- Updates or changes to the privacy policy

What data do we collect?

Category: Always

Below is an overview of the data we may collect:

- Non-identified and non-identifiable information that you provide during the registration process or that is collected through the use of our Services ("Non-Personal Data"). Non-personal information does not allow us to identify who collected it. Non-personal data that we collect consists mainly of technical and aggregated usage information
- Individually identifiable information, i.e. any information by which you can be identified or could reasonably be identified ("personal data"). Personal Data that we collect through our Services may include information that is requested from time to time, such as names, email addresses, addresses, phone numbers, IP addresses and more. If we combine personal data with non-personal data, we will treat it as personal data for as long as it is combined.

How do we collect data?

Category: Always

Below are the main methods we use to collect data:

- We collect data when you use our services. So when you visit our digital assets and use services, we may collect, record and store usage, sessions and related information.
- We collect data that you provide to us yourself, for example when you contact us directly via a communication channel (e.g. an email with a comment or feedback).
- We may collect data from third party sources as described below.
- We collect data that you provide to us when you log in to our services via a third party provider such as Facebook or Google.

Why do we collect this data?

Category: Always

We may use your data for the following purposes

- to provide and operate our Services;
- to develop, customize and improve our Services;
- to respond to your feedback, queries and requests and provide assistance
- to analyze request and usage patterns;
- for other internal, statistical and research purposes;
- to improve our data security and fraud prevention capabilities
- to investigate violations and enforce our terms and policies and to comply with applicable law, regulation or governmental request;
- to provide you with updates, news, promotional materials and other information related to our Services. For promotional emails, you can decide for yourself whether

you wish to continue receiving them. If not, simply click on the unsubscribe link in these emails.

Who do we share this data with?

Category: Always

We may share your data with our service providers in order to operate our services (e.g. storing data via third party hosting services, providing technical support, etc.).

We may also disclose your information in the following circumstances: (i) to investigate, detect, prevent or take action regarding illegal activities or other wrongdoing; (ii) to establish or exercise our rights of defense; (iii) to protect our rights, property or personal safety, or the safety of our users or the public; (iv) in the event of a change of control of us or one of our affiliates (by way of merger, acquisition or purchase of (substantially) all of its assets, etc.); (v) to collect and/or manage your information through authorized third party service providers (e.g., cloud service providers, as appropriate for business purposes); (vi) to share your information with authorized third party service providers (e.g., cloud service providers, as etc.); (v) to collect, hold and/or manage your information using authorized third party service providers (e.g. cloud service providers) as appropriate for business purposes; (vi) to work with third parties to improve your user experience. For the avoidance of doubt, please note that we may transfer, disclose or otherwise use non-personal data to third parties at our discretion.

Category: User has a blog or forum

Please note that our services enable social interactions (e.g. posting content, information and comments publicly and chatting with other users). Please note that any content or data you provide in these areas may be read, collected and used by others. We advise against posting or sharing information that you do not wish to make public. If you upload content to our digital assets or otherwise make it available as part of your use of a service, you do so at your own risk. We cannot control the actions of other users or members of the public with access to your data or content. You acknowledge and confirm that copies of your data may remain accessible even after they have been deleted from cached and archived pages or after a copy/storage of your content has been made by a third party.

Cookies and similar technologies

When you visit or access our Services, we authorize third parties to use web beacons, cookies, pixel tags, scripts and other technologies and analytics services ("Tracking Technologies"). These Tracking Technologies may allow third parties to automatically collect your data to

improve the browsing experience on our digital assets, optimize their performance and ensure a tailored user experience, as well as for security and fraud prevention purposes.

To find out more, please read our Cookie Policy.

Category: The user is NOT connected to an advertising service

We will not share your email address or other personal data with advertising companies or advertising networks without your consent.

Category: The user is connected to an advertising service, a campaign manager or Facebook Ads

We may serve advertising through our Services and our digital assets (including websites and applications that use our Services), which may also be tailored to you, such as ads based on your recent browsing behavior on websites, devices or browsers.

To deliver these ads to you, we may use cookies and/or JavaScript and/or web beacons (including transparent GIFs) and/or HTML5 Local Storage and/or other technologies. We may also use third parties, such as network advertisers (i.e., third parties that serve ads based on your website visits), to serve targeted ads. Third-party ad network providers, advertisers, sponsors and/or website traffic measurement services may also use cookies and/or JavaScript and/or web beacons (including clear GIFs) and/or Flash cookies and/or other technologies to measure the effectiveness of their ads and customize advertising content for you. These third-party cookies and other technologies are governed by the specific privacy policy of the third party and not this one.

Where do we store the data?

Category: Always

Non-personal data

Please note that our companies and our trusted partners and service providers are located around the world. We store and process any non-personal data we collect in different jurisdictions for the purposes set out in this Privacy Policy.

Category: User collects personal data

Personal Data

Personal Data may be maintained, processed and stored in the United States, Ireland, South Korea, Taiwan, Israel and, to the extent necessary for the proper provision of our Services and/or required by law (as further explained below), in other jurisdictions.

How long will the data be retained?

Category: Always

Please note that we will retain the information we collect for as long as necessary to provide our Services, comply with our legal and contractual obligations to you, resolve disputes and enforce our agreements.

We may correct, amend or delete inaccurate or incomplete data at any time at our discretion.

How do we protect the data?

Category: Always

The hosting service for our digital assets provides us with the online platform through which we can offer you our services. Your data may be stored via our hosting provider's data storage, databases and general applications. They store your data on secure servers behind a firewall and provide secure HTTPS access to most areas of their services.

Category: Users accept payments/eCom

All payment options offered by us and our hosting provider for our digital assets comply with the PCI-DSS (Payment Card Industry Data Security Standard) regulations of the PCI Security Standards Council. This is a collaboration between brands such as Visa, MasterCard, American Express and Discover. PCI-DSS requirements help to ensure the secure handling of credit card data (including physical, electronic and procedural measures) by our store and service providers.

Category: Always

Notwithstanding the measures and efforts taken by us and our hosting provider, we cannot and do not guarantee absolute protection and security of the data you upload, post or otherwise transmit to us or others.

For this reason, we encourage you to set strong passwords and, whenever possible, not to provide us or others with confidential information that you believe could cause you significant or lasting harm if disclosed. As e-mail and instant messaging are not considered secure forms of communication, we also ask you not to disclose confidential information via either of these communication channels.

How do we deal with minors?

Category: Users DO NOT collect data from minors

The Services are not intended for users who have not yet reached the legal age of majority. We will not knowingly collect data from children. If you are under the age of majority, you should not download or use the Services or provide us with any information.

We reserve the right to ask for proof of age at any time so that we can check whether minors are using our services. In the event that we become aware that a minor is using our Services, we may prohibit and block such users from accessing our Services and we may delete any information we hold about that user. If you have reason to believe that a minor has disclosed data to us, please contact us as explained below.

Category: Users collecting data from minors

Children can use our services. However, if they wish to access certain features, they may be required to provide certain information. The collection of some data (including data collected via cookies, web beacons and other similar technologies) may be automatic. If we knowingly collect, use or disclose information collected from a child, we will provide notice and obtain parental consent in accordance with applicable law. We will not condition a child's participation in an online activity on the child providing more contact information than is reasonably necessary to participate in that activity. We will only use the information we collect in connection with the services that the child has requested.

We may also use a parent's contact information to communicate about the child's activities on the Services. Parents may review information we have collected from their child, prohibit us from collecting further information from their child, and request that any information we have collected be deleted from our records.

Please contact us to view, update or delete your child's data. To protect your child, we may ask you to provide proof of your identity. We may deny you access to the data if we believe that your identity is questionable. Please note that certain data cannot be deleted due to other legal obligations.

Category: Always

We will only use your personal data for the purposes set out in the Privacy Policy and only if we are satisfied that:

- the use of your personal data is necessary to perform or enter into a contract (e.g. to provide you with the Services themselves or customer or technical support);
- the use of your personal data is necessary to comply with relevant legal or regulatory obligations; or
- the use of your personal data is necessary to support our legitimate business interests (provided that this is done at all times in a way that is proportionate and respects your data protection rights).

As an EU resident, you may:

- Request confirmation as to whether or not personal data concerning you is being processed and request access to your stored personal data and certain additional information;
- request to receive the personal data you have provided to us in a structured, commonly used and machine-readable format
- request the correction of your personal data stored by us
- request the erasure of your personal data;
- object to the processing of your personal data by us;
- request the restriction of the processing of your personal data, or
- lodge a complaint with a supervisory authority.

Please note, however, that these rights are not absolute and may be subject to our own legitimate interests and regulatory requirements. If you have general questions about the personal data we collect and how we use it, please contact us as set out below.

In the course of providing the Services, we may transfer data across borders to affiliates or other third parties and from your country/jurisdiction to other countries/jurisdictions around the world. By using the Services, you consent to the transfer of your data outside the EEA.

If you are located in the EEA, your personal data will only be transferred to locations outside the EEA if we are satisfied that an adequate or equivalent level of protection of personal data exists. We will take appropriate steps to ensure that we have appropriate contractual arrangements in place with our third parties to ensure that appropriate safeguards are in place so that the risk of unlawful use, alteration, deletion, loss or theft of your personal data is minimized and that such third parties act at all times in accordance with applicable laws.

Rights under the California Consumer Privacy Act

If you use the Services as a California resident, you may be entitled to request access to and deletion of your information under the California Consumer Privacy Act ("CCPA").

To exercise your right to access and delete your information, please see below for how to contact us.

Category: The website does not sell data of its users

We do not sell users' personal information for the purposes of the CCPA.

Category: Websites with a blog or forum

Users of the Services who are California residents and under the age of 18 may request and obtain removal of their posted content by sending an email to the address provided in the "Contact Us" section below. These requests must all be labeled "California Removal Request". All requests must include a description of the content you wish to have removed and sufficient information to allow us to locate the material. We will not accept notices that are

not labeled or properly submitted, and we may not be able to respond if you do not provide sufficient information. Please note that your request does not ensure that the material will be completely or comprehensively deleted. For example, material you have posted may be republished or re-posted by other users or third parties.

Updates or changes to the privacy policy

Category: Always

We may revise this Privacy Policy from time to time at our sole discretion, but the version posted on the Site will always be current (see the "Status" statement). We ask you to check this Privacy Policy regularly for changes. In the event of significant changes, we will publish a notice on our website. Your continued use of the Services following notification of changes on our website will constitute your acknowledgement and acceptance of the changes to the Privacy Policy and your agreement to be bound by the terms of those changes.

Contact Us

Category: Always

If you have general questions about the Services or the information we collect about you and how we use it, please contact us at

Name: EXTOLL GmbH

Address: Rheinvorlandstraße 5, 68159 Mannheim, Germany

E-mail address: general-data-protection-regulation@extoll.com

DISCLAIMER

The information contained herein does not constitute legal advice and should not be relied upon in isolation. Specific requirements regarding legal terms and guidelines may vary from state to state and/or jurisdiction to jurisdiction. As set out in our Terms of Use, you are responsible for ensuring that your Services are permitted by and comply with the law that applies to you.

To ensure that you are fully compliant with your legal obligations, we strongly recommend that you seek professional advice to better understand which requirements apply specifically to you.