

The EU General Data Protection Regulation (GDPR) at jacando

Our measures for compliance with the current GDPR

Table of contents

- GDPR implementation at jacando
- Principles
- Rights of the data subject
- Measures for responsible persons and contract processors

GDPR implementation at jacando

The basic regulation on data protection in the EU came into force on 25.05.2018. It protects the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data and the free movement of such data. The reasons for the implementation of the GDPR include the fundamental right to data protection, the harmonization of European data protection law, an equivalent level of protection despite national leeway and the guarantee of a high level of data protection despite increasing data exchange.

jacando is a GDPR compliant company

Even though jacando as a Swiss company does not belong to the EU, it is our duty and our concern, through our presence in Europe, to comply with the data protection rules of all our customers and to implement quality and security in all respects.

jacando is GDPR-compliant and fulfills all criteria of the basic data protection regulation, which came into force in May 2018. Since the handling of sensitive data is a fundamental element of our product strategy, we at jacando take data protection very seriously. Therefore, we offer our customers absolute transparency regarding

the technical and organizational measures we take to protect all data.

To ensure compliance with the law, jacando has an external data security officer who supports our company in this sensitive area. In addition, jacando has an internal team that is available to answer any questions regarding the GDPR.

In the following, we provide an overview of the different dimensions of the current general data protection regulation. In each case, we will point out in detail how jacando implements these legal guidelines. The formulation of the respective provisions is therefore based on the applicable wording of the law.

Principles

(Chapter 2 GDPR)

The second chapter of the GDPR focuses on the processing of personal data (Art. 5 and 6 GDPR). This includes the regulation that personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a manner incompatible with these purposes.

Therefore jacando works **exclusively** with the data agreed upon in the customer contract and treats these **extremely sensitively**. In addition, all personal data will be processed by jacando according to the GDPR in a manner that ensures adequate security, including protection against unauthorized or unlawful processing and against unintentional loss, destruction or damage through appropriate technical and organizational measures („integrity and confidentiality“). **In doing so, the responsible instance must provide evidence of compliance with the principles of data protection and is therefore liable to account.**

To comply with these guidelines, jacando relies on ISO 27001 certified servers.

For the processing of personal data, there must be a legal basis, i.e., for example, the consent of the customer or another legal obligation, which is defined in the customer contract with jacando. As a data processor, jacando has generated internal processes and structures that ensure GDPR-compliant work. Servers in the EU, especially in Germany and Switzerland, guarantee security for the data of all our customers. **A complete back-up is regularly created for all customer data and systems.**

jacando is always working on further developing its data protection and information security management system and adapting it to the current legal situation as well as customer needs. In addition, jacando emphasizes the GDPR-compliant data processing **in its employment contracts and internal company guidelines in order to sensitize employees to the importance of the required data processing.**

Rights of the data subject

(Chapter 3 GDPR)

Transparency and Information (Art. 12,13,14 GDPR)

- In the context of the GDPR jacando together with our data protection officer has developed a data protection declaration for our application. This allows every user to see which data is processed by us under his or her own responsibility, which third-party providers are used to providing the services, what we need this data for and what rights users have. Important: The personal data of your company administered in the jacando application are processed exclusively by the subcontractors mentioned in the data processing agreement. customer contract. The third party providers mentioned in the data protection declaration do not have access to this data.
- jacando's privacy policy can be viewed by every user on our homepage and is available in both German and English.
- In order to ensure that your use of jacando's recruiting functions fulfills your duty to inform regarding your applicants, we offer you the opportunity to link your own data protection declaration on your jacando career page.

Right of access by the data subject (Art. 15 GDPR)

- When using the jacando software, the individual employee is enabled to have direct access to his or her personal personnel file and other personal data available to the company about the employee at any time via their own user account. By means of these functions, which jacando offers, it becomes possible for our customers to **preserve the right of access towards their own employees.**
- Changes of the digital personnel file can be found in the employee history. All essential activities are also logged and stored in order to be able to verify access and changes to data. In case of irregularities, jacando is happy to provide its customers with these logs on request.

Right to rectification (Art. 16 GDPR)

- jacando offers its customers the possibility to individually define via **different user roles** which data can be viewed by employees and which can be processed independently by employees. Thus, even incorrect personal data can be changed by employees themselves or an immediate correction can be required.
- The employee himself or herself, therefore, has pre-selected editing rights and the respective **account administrator** has comprehensive rights.

**Right to erasure
(Art. 17 GDPR)**

- As soon as there is no longer any purpose for processing applicant and employee data, you as the client are obliged to **delete data that you no longer need**. This is done in consideration of possible legal storage obligations (see also Art. 18 GDPR). We support you with comprehensive functions within the application to simplify this process. Such as the **automated deletion of applicant data within the application**: To do this, activate the automatic deletion of applicant data in the recruiting settings. Thus all personal data of rejected or dismissed applicants will be irretrievably removed from the jacando application after the defined deadline. Anonymous metadata of applicants without personal reference will be preserved for your reporting.
- In case of termination of the business relationship with jacando AG, authorized persons of your company can request that jacando hands out all data in a machine-readable format. 30 days after the termination of the business relationship, the jacando account of your organization and all related data will be automatically and irretrievably deleted, which means that we comply with the **right to erasure**.

**Right to restriction
of processing
(Art. 18 GDPR)**

Regarding labor law, personnel files should in principle be kept for **up to three years after termination** of employment. Pursuant to Art. 18 GDPR, the employees concerned may request that the data be restricted for this purpose or in the event of incorrect data. In this way, they ensure that the data are not used or modified for further purposes.

Controller and Processor

(Chapter 4 GDPR)

Data protection by design and by default (Art. 25 GDPR)

With regard to the changed framework conditions caused by the GDPR, jacando has examined and adapted the entire application in order to be able to continue to guarantee customers legal data use. This includes, for example, the **standard restriction** of attributes which are transferred via our API, private calendar invitations for applicant interviews and feedback interviews as well as the possibility to deactivate any e-mail notifications for jacando accounts.

- Our presets are designed in a way that our customers can customize the system according to their individual needs.
- In order to ensure data protection-friendly settings and data protection through technology design on an ongoing basis, jacando has developed a system to implement legal guidelines into the product development process on an ongoing basis and to check the application at regular intervals.

Processor (Art. 28 GDPR)

As in the old law of the Federal Data Protection Act, data processing must always be carried out on the basis of a contract. In the context of the GDPR, this is referred to as the **data processing agreement**. jacando has fundamentally revised the data processing agreement and adapted it to the requirements of the GDPR. According to our work, we focus on the protection of the rights of the persons concerned from chapter 3 GDPR as well as the manifestation of corresponding control, reporting, and verification obligations. For more information, please contact your jacando contact person.

Records of processing activities (Art. 30 GDPR)

Article 30 of the GDPR states that companies must keep a register as a „responsible instance“ listing all processing activities that fall within the scope of responsibility of this company. In the case of this regulation, the size of the company is the decisive criterion for mandatory compliance, since companies with fewer than 250 employees are only affected by processing operations that pose a risk to the rights and freedoms of the data subjects or are not only carried out occasionally. Larger companies, i.e. companies with more than 250 employees, must generally comply with the aforementioned regulation. This applies to almost all processes in human resources and recruiting and therefore also applies when using the jacando Software.

Security of processing (Art. 32 GDPR)	In accordance with Article 32 of the GDPR, it is mandatory that you, as the responsible instance, and jacando, as the data processor commissioned to process personal data, implement appropriate technical and organizational measures (TOM) which take into account the state of the art, the implementation costs and the risk for the rights and freedoms of the persons concerned and ensure an appropriate level of protection. jacando has adapted its data protection security and information security and derived further technical and measures which guarantee the confidentiality, integrity, availability, and resilience of the systems and services. Further details can be found in our TOMs, which you are welcome to request.
Notification of personal data breach (Art. 33/34 GDPR)	In the event of a breach of personal data, reporting obligations to the supervisory authority must be fulfilled and the responsible instance and the persons concerned must be notified. To this case, jacando has set up appropriate reporting processes and documented the reporting channels in its TOMs.
Data protection officer (Art. 37/38/39 GDPR)	As a data processor who processes personal data, jacando has always been obliged to appoint a data protection officer. We rely on the services of MIP Consult. https://www.mip-consult.de/
Certification (Art. 42 GDPR)	At various points, the GDPR requires the provision of proof for responsible parties and data processors that all obligations, in particular, the implementation of suitable technical and organizational measures, have been fulfilled. The European member states have given themselves the task of defining corresponding rules of conduct (Art. 40 GDPR) and introducing a data protection-specific certification procedure (Art. 42 GDPR) in order to set a standard as proof. Despite the two-year transitional period, this has not yet taken place. jacando has recorded this separately in his TOM.
If you have further questions about data protection at jacando, please contact support@jacando.com	

