PRIVACY POLICY
BY USING Liliengerlach.com WEBSITE AND
Recruitment SERVICES
Effective 08/01/2018

The most important information is concise and comprehensive.

• The data of applicants - who are registered with us - will only be disclosed to our clients with their consent. We always consult on the phone in advance when a particular company or job opportunity arises.

• In case we contact applicants on their work phones, we do that very discreetly without mentioning the LGR name.

• Your data will only be forwarded - with your prior consent- to our clients whose vacancy is relevant to your job search.

• You can request forgotten, rectify, or access data; restrict processing; withdraw consent; and be kept informed about the processing of your data.

The detailed specifications of our privacy policy are as follows.

Detailed DATA PROCESSING INFORMATION

The operator of the Liliengerlach.com website (hereinafter: The Website), Gerlach Lilien Self-employed. Headquarters: 7441 – Austria, Pilgersdorf, Salmannsdorf 41., (hereinafter: LGR) informs the Users below about the General Data Protection Regulation 2016/679 of the European Parliament and of the Council on data processing on the Website and during the recruitment service provided by LGR. (Hereinafter referred to as the GDPR).

1.) Concepts

LGR : The Liliengerlach.com Website ("Website") is operated by the self-employed Lilien Gerlach. Headquarters: 7441 – Austria Pilgersdor, Salmannsdorf 41., who operates the website and provides employment agency services.
Website: All content and services available in the Liliengerlach.com domain.

Recruitment: Employer Job Ads

The totality of the services provided by LGR to promote it to the meeting of jobseekers to establish employment relationships, including the transfer of EU nationals to the home country and/or abroad and the transfer of foreign nationals to the destination country. This includes, but is not limited to, finding job seekers, collecting CVs, and database, even by posting an advertisement, as well as assessing the suitability of candidates, pre-screening candidates, selecting candidates, presenting to the Employer, presenting the Employer to the candidate, and checking references.

Employer: An employer with a contract relationship with LGR who is in a position looking for an employee, a candidate for the job, and uses LGR services to that end.

Job Ads: Online/offline advertisement for finding a candidate for a position determined by a particular employer.

Candidate: An individual applying for a job ad or directly contacted.

Visitor: Any natural person visiting the website who does not apply for a job but is browsing the website.

User: The common name of the Candidate and the Visitor.

General website terms of use:
The General Terms of Use of the Website, as published on the Website, which governs in detail how Users are authorised to access the Website and the services available through it, including Employment Services, use it.

2.) Purpose of the privacy policy

1. The Terms of Use of the Website are contained in the GTC, which shall apply to all matters not settled here. Use of the Website and its Services: A contract is entered between LGR and the User under the terms and conditions of the Website. In this Privacy Statement, LGR provides users with detailed information regarding the processing of personal data through the Website and its Employment Services, in accordance with the law.

2. LGR shall be deemed to be a data controller for data processing on the website. LGR shall also be deemed to be a Data Controller with respect to Candidate Personal Data processed by the Labour Exchange and transmitted by Employers to LGR when managing such Candidates' data, not on behalf of or behalf of the Employer employing them, such as its database. Besides, all Employers contracted by LGR to whom LGR transmits the Candidates' data, curriculum vitae, and the application form shall be deemed to be a Data Controller. The LGR and Employers are separate data controllers, each of whom carries out its own data management activities, as defined in its privacy policy. However, LGR is a data processor acting on behalf of employees when processing Candidate Data solely on behalf of employees and not for storage in its database.

3. Employers, as independent data controllers, are required to carry out their own data management in accordance with the law and to inform candidates of their data management in their data management information. LGR is not responsible for the accuracy, completeness, or lawfulness of this Employer data.

Management Information; LGR is solely responsible for the legality of its own data management.

3.) Purpose of the website

1. Users may apply for a particular job by submitting their CV and other documents to LGR.

2. The Services of the Website and Employment Services shall be available only to individuals over 18 years of age. If you submit a different resume or apply for a job on behalf of a user on behalf of another user, you warrant that you have the full consent of that third party and the processing and transfer of your data.

3. The User is responsible for the data provided by the Users and the content uploaded by them, and LGR disclaims any liability.

4.) How does the Privacy Notice apply to the User?

1. By accessing the website and using its features, users automatically acknowledge, without further notice, the sections of this Privacy Policy relating to the operation of the website.
2. For job placement, see 6.1.2.)

5.) Who and how can I modify the privacy policy and where does the LGR publish it?

1. At any time, LGR may unilaterally modify this Privacy Policy. LGR will publish changes to this Privacy Statement by displaying the Consolidated Privacy Statement on the Website under a separate Privacy Policy. Users are requested to read the privacy policy carefully each time they visit the site.

2. This Privacy Statement is permanently available on the website. Users may open, view, print, save, but not modify this Privacy Statement on the Website; only LGR is authorised to do so.

6.) What personal data do we process, how long do we use it, and for what authorization?

1. Voluntary informed consent of the user to the data management according to Article 6 (1) (a) of the GDPR ("Consent");

2. according to Article 6 (1) (b) of the GDPR, data processing is necessary for the performance of a contract to which the User, as a party, is a party,

3. according to Article 6 (1) (c) of the GDPR, data processing is necessary for the performance of a legal obligation to which the data controller is subject (such as accounting, bookkeeping or "legal compliance")

4. According to Article 6 (1) (f) of the GDPR, data processing is necessary to pursue the legitimate interests of the controller or third party. The User's natural personal data (name, birth name, mother's birth name, place, and date of birth) and address can be managed without the consent of the user; for billing, charging, and enforcing any related fees, and without the user's consent, the user's natural identity, address, date, duration, and location of use of the information society service.

5. Employers, as independent data controllers, are obliged to carry out their own data management in accordance with the law and to inform candidates of their data management in their data management information. LGR is not responsible for the accuracy, completeness, or lawfulness of this Employer Data Management Information; it is solely responsible for the legality of its data management.

6. At any time, LGR may unilaterally modify this Privacy Policy. LGR will publish changes to the Privacy Statement in a consolidated version of the Privacy Statement on the Website under a separate Privacy section.

7. Data Management for Anonymous Job Ads

The LGR may also, on behalf of Employers, publish Job Ads in which Employers do not disclose their identity and so Candidates will not know which Employer they are applying for (Anonymous Job Ad).

In the case of such Anonymous Job Ads, the LGR will, to the fullest extent possible, protect the rights and interests of candidates by informing candidates of the employee's identity in the application process prior to submitting an application. Thus, Candidate can decide whether to request the transfer of your data to that Employer.

In order to protect the business secrets of the Employers, Candidates are obligated to maintain strict confidentiality and confidentiality with respect to the Employer posting the Anonymous Job, its identity, and name, and may not disclose it directly or indirectly to anyone without the prior permission of the Employer.

6.2.) Manage customer contact information

Category concerned	**Category of** managed data	**Source of** Data	**Purpose of Data**	**Legal basis for** data management	**Duration of data** storage, date of deletion
The person who contacted Customer support	Name	Given by the Customer	Complaint management	Article 6 (1) GDPR Point: Legal interest	5 years
	Phone	Given by the Customer	Complaint management	Article 6 (1) GDPR Point: Legal interest	5 years
	E-mail	Given by the Customer	Complaint management	Article 6 (1) GDPR Point (f): Legal interest	5 years
	Personal	Given by	Complaint	Article 6 (1)	5 years

	information provided in the complaint	the Customer	management	GDPR Point (f): Legal interest	

The name, e-mail address, and telephone number are mandatory for Customer Support Identification and further administration purposes, without which LGR will not be able to receive, investigate, or take further action. The provision of personal information necessary for Identification, Complaint Investigation, Further Administration, and Legal and Claim Enforcement arising from any complaint is limited to the Candidate and LGR's legitimate interest. This does not violate or endanger the other person's fundamental rights and freedoms. The time required for handling and retaining customer contact information is the same as the general 5 years civil statute of limitations; retention of data within this limitation period is necessary for the enforcement of rights and claims. Please be advised that you may object to Customer Service, and Complaint Management for purposes of legitimate interest, and if you do so, subject to any applicable legal requirements, will not be processed further.

7.) Who manages your personal information and who has access to it?

7.1.) Data Manager

The data specified in Section 6 is the Data Manager of the LGR, and its contact details are as follows:

Gerlach Lilien Self-employed

Headquarters: 7441-Österreich Pilgersdorf, Salmannsdorf 41.
GISA- Zahl: 32792164
Phone: +436764946323
Email: office@liliengerlach. com

LGR data is accessed by LGR employees to the extent strictly necessary to carry out their work.
Access to your data is governed by strict internal rules.

7.2.) Data Processors

We use different companies with whom we have a data-processing contract to manage and store your data. The following data processors processes the data.

Name of data processors	Data processing activities	Scope of managed data
Czar Milan self-employed (7762 Pécsudvard, Tancsics Mihaly u. 13)	Providing Internet web hosting, Virtual Private Server, Mail server services, Hardware, software maintenance, and support.	LGR recruitment data uploaded to ATS software: CV data, ID number, name, e-mail address, phone number, position applied for, tax number, address, year of birth, last communication date, registration date, status (active/passive), expected payment and other requirements, qualification area, level, name, spoken language type, level, work experience area, position level, number of years, ideal workspace name, position level, location, application date, company feedback, email address, name, telephone number, name of the employer, the position of the public client, potential customer contacts.
3Gteam Kft	Maintenance of software on file and mail server, VPS service	Candidates uploaded to ATS software (CV, ID number, name, e-mail address, telephonenumber, position applied for, tax number, address, year of birth, last communication date, registration date, status (active / passive), expected salary and other demands, qualifications, area, level, name, spoken language, type, level, work experience the area, position level, number of years, ideal

1114 Budapest, Horánszky u. 23.		workspace name, location, and position level. Application date, company feedback) E-mail address, name, phone number, name of employer, position of contracting authorities, customer who contacted customer support.

8.) Who do we forward your personal information to?

In addition to the data processors listed above, your personal information will be forwarded to employees who have entrusted us with the employment services.

Category the transmitted data: LGR contracted clients

Type of recipient of the data transfer

Candidates for LGR recruitment (CV, ID number, name, email address, phone number, position applied for, home address, year of birth, expected salary and other requirements, degree, level, name, type of language spoken), level, work experience area, position level, number of years, ideal workspace name, position level, location)

The purpose of the above transfer is to provide LGR with Employees contracted to provide employment services; LGR will send Candidate CVs and other data collected by LGR in the Recruitment process and Employers will, where appropriate, find a Candidate for a given position—find a job with a job offer and sign a contract with him. Following the transfer of data to the Employer, the Employer shall be considered an independent Data Manager and shall act following its own data management rules and information.

9.) How do we ensure the security of your data?

We have a comprehensive information security policy to ensure the security of the data and information we handle, which is mandatory for all our employees and subcontractors, and is known and applied by all of our employees and subcontractors. We regularly train our employees on data and information security requirements.

9.1.) Data security in IT infrastructure

1.Personal data on the servers of the VPS provider to which our employees and subcontractors have access under strict rights management rules. Occasionally, our IT systems are tested and audited to ensure that we maintain data and IT security.

2.Office workstations are password-protected, and foreign media can only be used after automatic virus and malware filtering.

3.Regular and continuous protection against malicious software is provided for all systems and components of the LGR.

4.In the design, development, testing, and operation of our programs, applications, and tools, we prioritise security features separately.

5.Information system access keys (e.g. passwords) are stored encrypted, and protection of system security data (e.g. passwords, privileges, logs) is ensured by granting access privilege

9.2.) Data security in communication

1.We use SSL/TSL encryption for messages and files transmitted electronically. To satisfy the requirement of secure data exchange, we ensure data integrity for both (communication) control and user data. Error detection and correction procedures were used to prevent data loss and damage.

2.The protection we apply detects the occurrence of unauthorised intrusion, alteration, and intrusion. We prevent data loss and damage through error detection and correction procedures and ensure that they are not denied.

3.In the case of a network used for data transmission, we shall ensure that unauthorised access and interception are prevented in a manner appropriate to the level of security

9.3.) Data security during software development and programming

1.During the development of our website and systems, we incorporated data protection and data security requirements into the design process, which we continuously ensured during development.

2.During software development, we separate the developer/test environment from the production environment, and in the course of testing, personalise personal data as much as possible.

3.In programming, we adhere to the basic requirements of secure coding, employ platform and program language-dependent techniques to eliminate typical vulnerabilities and follow the latest industry recommendations for code review.

4.We continually follow the identification of newly discovered vulnerabilities; our developers regularly follow industry data security recommendations and employ programming techniques to avoid typical bugs. Completed code verification is performed according to the principles of secure encryption, and changes are properly documented

9.4.) Data security during records management.

We also complied with the data security requirements set out in our recording policy. The records are handled by written authorization levels and by the security rules applicable to each

document confidentiality. We have detailed and strict rules regarding the destruction, storage, and extraction of records.

9.5.) Physical Data Security

1.To ensure physical data security, we ensured that our doors and windows were properly locked and protected.

2.Paper-based personal data documents should be placed in a locked security cabinet accessible to a limited number of people with appropriate access control.

3.Media storage rooms are designed to provide adequate security against unauthorised or violent intrusion, fire, or natural disasters. Media used for data transfer, backup, and archiving can only be stored securely in a closed place.

10.) What do we do if a privacy incident exists?

By law, we will report the data protection incident to the supervisory authority within 72 h of becoming aware of it and maintain records of the data protection incidents. We will also notify the affected users in the cases specified by law.

11.) When and how will we amend this Privacy Statement?

If the scope of the data processed and other circumstances of data management change, this Privacy Policy will be modified and published on the www.liliengerlach.com website within 30 days per the provisions of the GDPR. In all cases, please read the privacy policy changes carefully, as they contain important information about the management of your personal information