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

The most important information is in a presented concise and comprehensive way:

• The data of applicants - who are registered with us - will only be disclosed to our clients with their consent. We always consult in advance on the phone when a particular company and/or job opportunity arises.
• In case we contact applicants on their work-phone, we do that always very discreetly without mentioning the LGR name.
• Your data will only be forwarded - with your prior consent- to our client's whose vacancy is relevant to your job search.
• You can request to be forgotten, to rectify or access data, to restrict processing, to withdraw consent, to be kept informed about the processing of your data.

The specifications of our privacy policy you can find below in details:

Detailed DATA PROCESSING INFORMATION

The operator of the Liliengerlach.com website (hereinafter: the Website), Gerlach Lilien Selfemployed. Headquarters: 7441 – Österreich Pilgersdor, 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.comWebsite ("Website") is operated by Gerlach Lilien ev. Headquarters:7441 – Österreich Pilgersdor, Salmannsdorf 41., who operates the Website and provides employment agency services.
Website	All content and services available under the Liliengerlach.com domain.
Recruitment	The totality of the services provided by LGR to promote it the meeting of jobseekers and 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, 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, checking references.
Employer	An employer with a contract relationship with LGR who is in a positionis 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	A natural person 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.
Website general term of use	The General Terms of Use of the Website, as published on the Website, which governs in detail how Users are authorized to access the Website and including the services available through it, including the Employment Services, use it.

2.) What is the 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 into 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 concerning for data processing on the Website. LGR shall also be deemed to be a Data Controller in respect of Candidate Personal Data processed by Labor 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, the application form shall be deemed to be a Data Controller. The LGR and the 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 and behalf of Employers when processing Candidate Data solely on behalf of such Employers 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.) What is the 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 the Employment Services shall be available only to persons 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 the features of the Website, 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?

3. The LGR may at any time 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.

4. 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 authorized 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 for the pursuit of the legitimate interests of the controller or of a third party (hereinafter:
5. Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services. 13 / A. § data processing license, according to which the User's natural personal data (name, birth name, mother's birth name, place and date of birth) and address of the User 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, and date, duration, and location of use of the information society service (hereinafter referred to as Section 13 / A.).
6. Employers, as independent data controllers, are obliged to carry out their own data management in accordance with the law and to inform the 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.
7. LGR may at any time 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 the separate Privacy section.

6.1.) Data management in Recruitment

6.1.1.) This Privacy Statement applies to each of the following recruitment services:

a.) if you apply for a Job Ad by emailing the Candidate's CV

b.) if the Candidate in the LGR Database is contacted by the LGR for a specific Job Ad

c.) if the Candidate is found and searched for by LGR in another recruitment database or social media for a specific Job Ad

d.) if the Candidate is listed in LGR's on database not for the specific purpose of applying for a Job Ad, but for future offers (Database Storage).

6.1.2.) The LGR obtains Candidates' CVs and personal information from multiple sources:

a.) The Candidate will provide his / her data through the Website by filling in the form and submitting his / her CV, in which case the data will be provided by the Candidate as a person concerned.

b.) The Candidate's Curriculum Vitae and Data Legally, LGR obtains it from the database of other recruitment agencies and job placement portals based on its contract with these job placement portals and recruitment agencies.

c.) Some Candidate Data by LGR itself, based on its research, from old employers, such as reference data.

d.) If you apply for a job by email (job@liliengerlach.com), you must declare that you are familiar with the privacy policy and consent to the management of your information.

6.1.3.) Type, source, purpose, legal basis and duration of the data processing

Sources of data other than those listed above are listed separately in the data management table below so that Candidates are always aware of where their data is obtained from LGR and what their source is. In the table below, we also indicate for each data type the purpose and legal basis for which we treat your data.

Affected Category	Category of managed data (* = required)	Data source	Purpose of data management	Legal basis for data management	Duration of data storage
Jobseekers Managed by Recruitment Services (Candidates)	CV Information	Candidate Job ortals eg: CV Online, Profession. Monster. Jobline.	Recruitment Job Offer Contact Identification	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	ID	Data manager	Identification	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.

	Name*	Candidate	Recruitment Job Offer Kapcsolattartás Identification	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	e-mail*	Candidate	Recruitment Job Offer Kapcsolattartás Identification	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	Phone*	Candidate	Recruitment Job Offer Kapcsolattartás Identification	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	Position Applied for	Candidate	Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	Address	Candidate	Recruitment Job Offer Kapcsolattartás Identification	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	Birth of Date*	Candidate	Recruitment Job Offer Identification	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	last communication date	Data Manager	Identification	Article 6 (1) GDPR Point (a): the data subject has given his consent to the	Until recruitment for that position is completed, but for up to 1 year.

				processing of his personal data	In case of separate consent for database storage: 2 years.
	date of registration	Data Manager	Identification	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	staus (active/passive)	Data Manager	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	salary of other requirements*	Candidate	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	name, area and level of education*	Candidate	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	oral and writing language ability	Candidate	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	The area, position, level, number of years of working experience *	Candidate	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.

	Ideal job, level of the position and location.	Candidate	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	Application date	Candidate	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	Employer feedback about the position you applied for	Data Manager	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	Nationality	Candidate	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	publications, presentations, projects	Candidate	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	education	Candidate	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	awards, honors	Candidate	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.

	References	Candidate or Data Manager	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	Social Media Daten	Data Manager	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	During the interview, personality and behavioural characteristics needed for evaluating the suitability	Data Manager	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. In case of separate consent for database storage: 2 years.
	Professional test answers and results	Candidate	Recruitment Job Offer	Article 6 (1) GDPR Point (a): the data subject has given his consent to the processing of his personal data	Until recruitment for that position is completed, but for up to 1 year. jelölIn case of separate consent for database storage: 2 years.

6.1.5.) How do we use public information available on social media interfaces?

When applying for a Candidate Job Ad, the LGR can view the profile, activity, activity, posts, posts, comments made on Candidate Community Media interfaces, such as Facebook, LinkedIn, to determine whether Candidate is eligible for the position in the Job Ad. LGR will only view publicly available information about Candidate on social media platforms, and will not search Candidates in closed groups or other non-restricted or restricted public places. The LGR does not save or store Candidate community media profiles, but you may make a note of the data you view and view on Candidate and store it on paper and electronically in a database of Candidate.

LGR does not handle sensitive or sensitive information about Candidate based on social media profile information either. The LGR will only view relevant job listing information on Candidates on the social media site.

6.1.6.) What do we use in our database for Candidate data collected from different sources?

The information provided by Candidate in your resume and the data collected by LGR on Candidates, such as LGR records of publicly available data on social media interfaces, Candidate data collected from other sources,

and interviews with CandidateLGR LGR observes behavioural, personality traits, and results of professional tests completed at LGR. LGR interconnects and assigns to Candidate. The data set thus obtained shall be used by LGR for the following purposes:

a.) send personalized Job Ads to Candidate

b.) a Candidate Recommendation to the Employer contracted by LGR

c.) compiles statistics from the data for own use and for external customers in an anonymized manner

d.) categorize the Candidates in their electronic database on the basis of the managed data.

LGR does not use automated tools to evaluate Candidate data without human intervention, nor does it use software or other automated tools to make decisions about Candidates based on the analysis of their data or predictions derived therefrom. As a result, the above data linking does not constitute automated profiling, nor does it require the explicit consent of Candidateek.

6.1.8.) Notify Candidate of the success of your application

The candidate will be informed by the Employer whether or not the Employer has recruited the job, and LGR is not responsible for sending this information.

6.1.9.) Granting and withdrawal of consent

Candidates give their voluntary consent to the above-mentioned management of their data by actively submitting their application to the Job Ad on the form on the Website and by ticking the consent checkbox. Candidates may revoke their consent to data management at any time by sending an email to job@liliengerlach.com with the required details: name, date of birth and email address to enable LGR to identify which you must delete your candidate information. Also, after registering and logging in to the Website, Candidates may delete their account by double-clicking on the Delete Account button in their account on the Website, in which case their data from other sources will be automatically deleted and they are no longer managed by LGR.

In the event of withdrawal of consent, the LGR will delete the data handled by the Candidate for all LGRs, as provided by the Candidate. The obligation of deletion covers both electronic and paper-based data.

6.1.10.) Duration of data management, data management for project and database purposes

The LGR, if Candidate applies for a particular Job, will process your Candidate Information during the Recruitment Process related to this Job, and will delete all Candidate data at the same time you complete the Recruitment Process. If the Recruitment Process is delayed and takes more than one year, LGR will process Candidate data for a maximum of one year after submission, upon expiration of which it will ask Candidate again whether it intends to extend the processing of the Recruitment Process for more than one year. If you do not respond to the Candidate within 30 days or if you do not wish to extend the Candidate the Data Management Period, the LGR will delete your Candidate Data.

LGR may forward your Candidate Information and CV to a particular Job Administ to another Employer and manage it in its database for future job offers if you have consented to it on the Candidate Site. The LGR will ask Candidate for specific consent. If you have given Candidate's consent, LGR will be entitled to manage your Candidate Information in its database for such purposes for a further 2 years. The reason for the 2 years is that the LGR must ensure the accuracy and timeliness of the data provided by Candidate and collected and processed by Candidate, and after 2 years this can no longer be guaranteed, the data may become outdated and may lose its relevance. Before 2 years LGR may contact Candidates for another 2 years of data management consent.

6.1.11.) 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 Employer's identity in the application process prior to submitting an application. So, 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 under an obligation to maintain strict confidentiality and confidentiality with respect to the Employer posting the Anonymous Job, its identity and name, and may not disclose or 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 (f): Legal interest	5 years
	Phone	Given by the Customer	Complaint management	Article 6 (1) GDPR Point (f): Legal interest	5 years
	E-mail	Given by the Customer	Complaint management	Article 6 (1) GDPR Point (f): Legal interest	5 years
	Personal information provided in the complaint	Given by the Customer	Complaint management	Article 6 (1) GDPR Point (f): Legal interest	5 years

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, which 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 the Customer Service, 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 Selfemployed

• 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 process their data:

Name of datap rocessors	Data processing activities	Scope of managed data
Czar Milan selfemployed (7762 Pécsudvard, Tancsics Mihaly u. 13)	Providing Internet web hosting, Virtual Private Server, Mail server services	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)
	Hardware, software maintenance and support	Daten werden automatisch von Website-Besuchern gesammelt
		Name und E-Mail-Adresse der Newsletter-Abonnenten
		E-Mail-Adresse, Name, Telefonnummer, Name des Arbeitgebers, Position des öffentlichen Auftraggebers, potenzielle Kundenkontakte
3Gteam Kft **1114 Budapest, Horánszky u. 23.**	Maintenance of software on file and mail server, VPS service	andidates uploaded to ATS software (CV, ID number, name, e-mail address, telephone number, 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 workspace name, location and level of the position

		application date, company feedback)
		E-mail address, name, phone number, name of employer, position of contracting authorities, potential customer contacts
		Customer who contacted the customer support
		name, email address of the newsletter signup
Google LLC (1600 Amphitheatre Pkwy Mountain View, California 94043; USA)	Google Analytics, Google adwords, Google remarketing services	About Customers Website Visitors in Google Analytics, Google Adwords data collected
Facebook, Inc. (1601 Willow Road, Menlo Park, California 94025; lperry@fb.com, USA)	Providing Facebook remarketing service (profiling, advertising, analytics & measurement, behavioral advertising)	Website visitors on Facebook Pixel data collected by
The Rocket Science Group LLC d/b/a MailChimp (székhely: Georgia 675 Ponce De Leon Ave NE, Suite 5000 Atlanta, Georgia 30308)	Operation of newsletter sending system	name and e-mail address of Newsletter sign-up

Among the data processors employed is MailChimp, a US-based The Rocket Science Group LLC, located at 675 Ponce De Leon Ave NE, Suite 5000 Atlanta, Georgia, Facebook, Inc. (1601 Willow Road, Menlo Park, California) 94025; lperry@fb.com, USA) and Google, LLC. (1600 Amphitheater Pkwy Mountain View, California 94043; USA) is listed in the European Commission Compliance Decision according to Article 45 of the GDPR and Commission Implementing Decision 2016/1260 and the US-EU Privacy Shield List established pursuant thereto. the transfer of data to third countries outside the European Union shall not be considered as such and shall not require the specific consent of the data subjects and shall not be permitted under Article 45 of the GDPR. These companies have undertaken to comply with the GDPR.

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

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

The type of recipient of the data transfer	Category the transmitted data
LGR contracted clients	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 Candidates CVs and other data collected by LGR in the Recruitment process and Employers will, where appropriate, find 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.

11.) 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 and train our employees on data and information security requirements.

11.1.) Data security in IT infrastructure

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

2. Office workstations are password-protected, 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 prioritize security features separately.

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

11.2.) Data security in communication

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

2. The protection we apply detects the occurrence of unauthorized 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 unauthorized access and interception are prevented, in a manner appropriate to the level of security.

11.3.) Data security during software development and programming

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

2. During software development, we separate the developer/test environment from the production environment, and in the course of testing, we personalize 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.

11.4.) Data security during records management

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

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

11.5.) Physical Data Security

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

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

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

12.) What do we do if we have a privacy incident?

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

13.) 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 on www.liliengerlach.com website within 30 days in accordance with 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.