HealthAI Privacy Policy

Preamble

With the following privacy policy we would like to inform you which types of your personal data (hereinafter also abbreviated as "data") we process for which purposes and in which scope. The privacy statement applies to all processing of personal data carried out by us, both in the context of providing our services and in particular on our websites, in mobile applications and within external online presences, such as our social media profiles (hereinafter collectively referred to as "online services").
The terms used are not gender-specific.
Last Update: 21. December 2023

Table of contents

- Job Application Process
- Cloud Services
- Newsletter and Electronic Communications
- Commercial communication by E-Mail, Postal Mail, Fax or Telephone
- Surveys and Questionnaires
- Web Analysis, Monitoring and Optimization
- Profiles in Social Networks (Social Media)
- Plugins and embedded functions and content
- Management, Organization and Utilities

Controller

I-DAIR Foundation
CEO Dr. Ricardo Baptista Leite
COO Anne Hassberger
Rue Varembé 7
1202 Geneva, Switzerland

E-mail address:
contact@healthai.agency

Contact information of the data protection officer

For questions you can contact our data protection advisor:

PlanSec AG
Dieter Huber
Sinserstrasse 67
6330 Cham, Switzerland

Email: mail@plansec.ch
Web: https://www.plansec.ch

Overview of processing operations

The following table summarises the types of data processed, the purposes for which they are processed and the concerned data subjects.

Categories of Processed Data

- Inventory data.
- Payment Data.
- Contact data.
- Content data.
- Contract data.
- Usage data.
- Meta, communication and process data.
- Job applicant details.
- Images and/ or video recordings.

Categories of Data Subjects

- Customers.
- Employees.
- Prospective customers.
- Communication partner.
- Users.
- Job applicants.
- Members.
- Business and contractual partners.
- Participants.
- Persons depicted.

Purposes of Processing

- Provision of contractual services and fulfillment of contractual obligations.
- Contact requests and communication.
- Security measures.
- Direct marketing.
- Web Analytics.
- Office and organisational procedures.
- Conversion tracking.
- Managing and responding to inquiries.

- Job Application Process.
- Server monitoring and error detection.
- Feedback.
- Marketing.
- Profiles with user-related information.
- Provision of our online services and usability.
- Information technology infrastructure.

Relevant legal bases

Relevant legal bases according to the GDPR: In the following, you will find an overview of the legal basis of the GDPR on which we base the processing of personal data. Please note that in addition to the provisions of the GDPR, national data protection provisions of your or our country of residence or domicile may apply. If, in addition, more specific legal bases are applicable in individual cases, we will inform you of these in the data protection declaration.

- **Consent (Article 6 (1) (a) GDPR)** - The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
- **Performance of a contract and prior requests (Article 6 (1) (b) GDPR)** - Performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- **Legitimate Interests (Article 6 (1) (f) GDPR)** - Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.
- **Job application process as a pre-contractual or contractual relationship (Article 6 (1) (b) GDPR)** - If special categories of personal data within the meaning of Article 9 (1) GDPR (e.g. health data, such as severely handicapped status or ethnic origin) are requested from applicants within the framework of the application procedure, so that the responsible person or the person concerned can carry out the obligations and exercising specific rights of the

controller or of the data subject in the field of employment and social security and social protection law, their processing shall be carried out in accordance with Article 9 (2)(b) GDPR , in the case of the protection of vital interests of applicants or other persons on the basis of Article 9 (2)(c) GDPR or for the purposes of preventive health care or occupational medicine, for the assessment of the employee's ability to work, for medical diagnostics, care or treatment in the health or social sector or for the administration of systems and services in the health or social sector in accordance with Article 9 (2)(d) GDPR. In the case of a communication of special categories of data based on voluntary consent, their processing is carried out on the basis of Article 9 (2)(a) GDPR.

Relevant legal basis according to the Swiss Data Protection Act: If you are located in Switzerland, we process your data based on the Federal Data Protection Act (abbreviated as "Swiss DPA"). This also applies if our processing of your data otherwise affects you in Switzerland and you are affected by the processing. The Swiss DPA does not generally provide that a legal basis for the processing of personal data must be stated (unlike, for example, the GDPR). We process personal data only when the processing is lawful, is conducted in good faith, and is proportionate (Article 6 (1) and (2) of the Swiss DPA). Furthermore, we only collect personal data for a specific purpose that is recognisable to the person concerned and process it only in a manner that is compatible with these purposes (Article 6 (3) of the Swiss DPA).

Reference to the applicability of the GDPR and the Swiss DPA: These privacy notices serve both to provide information in accordance with the Swiss Federal Act on Data Protection (Swiss DPA) and the General Data Protection Regulation (GDPR).

Security Precautions

We take appropriate technical and organisational measures in accordance with the legal requirements, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, in order to ensure a level of security appropriate to the risk.

The measures include, in particular, safeguarding the confidentiality, integrity and availability of data by controlling physical and electronic access to the data as well as

access to, input, transmission, securing and separation of the data. In addition, we have established procedures to ensure that data subjects' rights are respected, that data is erased, and that we are prepared to respond to data threats rapidly. Furthermore, we take the protection of personal data into account as early as the development or selection of hardware, software and service providers, in accordance with the principle of privacy by design and privacy by default.
TLS/SSL encryption (https): To protect the data of users transmitted via our online services, we use TLS/SSL encryption. Secure Sockets Layer (SSL) is the standard technology for securing internet connections by encrypting the data transmitted between a website or app and a browser (or between two servers). Transport Layer Security (TLS) is an updated and more secure version of SSL. Hyper Text Transfer Protocol Secure (HTTPS) is displayed in the URL when a website is secured by an SSL/TLS certificate.

Transmission of Personal Data

In the context of our processing of personal data, it may happen that the data is transferred to other places, companies or persons or that it is disclosed to them. Recipients of this data may include, for example, service providers commissioned with IT tasks or providers of services and content that are embedded in a website. In such cases, the legal requirements will be respected and in particular corresponding contracts or agreements, which serve the protection of your data, will be concluded with the recipients of your data.

International data transfers

Data Processing in Third Countries: If we process data in a third country (i.e., outside the European Union (EU) or the European Economic Area (EEA)), or if the processing is done within the context of using third-party services or the disclosure or transfer of data to other individuals, entities, or companies, this is only done in accordance with legal requirements. If the data protection level in the third country has been recognized by an adequacy decision (Article 45 GDPR), this serves as the basis for data transfer. Otherwise, data transfers only occur if the data protection level is otherwise ensured,

especially through standard contractual clauses (Article 46 (2)(c) GDPR), explicit consent, or in cases of contractual or legally required transfers (Article 49 (1) GDPR).
Furthermore, we provide you with the basis of third-country transfers from individual third-country providers, with adequacy decisions primarily serving as the foundation. "Information regarding third-country transfers and existing adequacy decisions can be obtained from the information provided by the EU Commission: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection_en.
EU-US Trans-Atlantic Data Privacy Framework: Within the context of the so-called "Data Privacy Framework" (DPF), the EU Commission has also recognized the data protection level for certain companies from the USA as secure within the adequacy decision of 10th July 2023. The list of certified companies as well as additional information about the DPF can be found on the website of the US Department of Commerce at https://www.dataprivacyframework.gov/. We will inform you which of our service providers are certified under the Data Privacy Framework as part of our data protection notices.
Disclosure of Personal Data Abroad: In accordance with the Swiss Data Protection Act (DSG), we only disclose personal data abroad when an appropriate level of protection for the affected persons is ensured (Art. 16 Swiss DSG). If the Federal Council does not determine that there is an adequate level of protection (list of states: https://www.bj.admin.ch/bj/de/home/staat/datenschutz/internationales/anerkennung-staaten.html), we implement alternative security measures. These measures may include international agreements, specific guarantees, data protection clauses in contracts, standard data protection clauses approved by the Federal Data Protection and Information Commissioner (FDPIC), or internal company data protection regulations previously recognised by the FDPIC or a competent data protection authority of another country.
Under Art. 16 of the Swiss DSG, exceptions can be made for the disclosure of data abroad if certain conditions are met, including the consent of the affected person, contract execution, public interest, protection of life or physical integrity, publicly made data or data from a legally provided register. Such disclosures always comply with the legal requirements.

Use of Cookies

Cookies are small text files or other data records that store information on end devices and read information from the end devices. For example, to store the login status in a user account, the contents of a shopping cart in an e-shop, the contents accessed or the functions used. Cookies can also be used for various purposes, e.g. for purposes of functionality, security and convenience of online offers as well as the creation of analyses of visitor flows.

Information on consent: We use cookies in accordance with the statutory provisions. Therefore, we obtain prior consent from users, except when it is not required by law. In particular, consent is not required if the storage and reading of information, including cookies, is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user. Essential cookies usually include cookies with functions related to the display and operability of the onlineservice, load balancing, security, storage of users' preferences and choices or similar purposes related to the provision of the main and secondary functions of the onlineservice requested by users. The revocable consent will be clearly communicated to the user and will contain the information on the respective cookie use.

Information on legal bases under data protection law: The legal basis under data protection law on which we process users' personal data with the use of cookies depends on whether we ask users for consent. If users consent, the legal basis for processing their data is their declared consent. Otherwise, the data processed with the help of cookies is processed on the basis of our legitimate interests (e.g. in a business operation of our online services and improvement of its usability) or, if this is done in the context of the fulfillment of our contractual obligations, if the use of cookies is necessary to fulfill our contractual obligations. For which purposes the cookies are processed by us, we do clarify in the course of this privacy policy or in the context of our consent and processing procedures.

Retention period: With regard to the retention period, a distinction is drawn between the following types of cookies:

- **Temporary cookies (also known as "session cookies"):** Temporary cookies are deleted at the latest after a user has left an online service and closed his or her end device (i.e. browser or mobile application).

- **Permanent cookies**: Permanent cookies remain stored even after the terminal device is closed. For example, the login status can be saved, or preferred content can be displayed directly when the user visits a website again. Likewise, user data collected with the help of cookies can be used for reach measurement. Unless we provide users with explicit information about the type and storage duration of cookies (e.g., as part of obtaining consent), users should assume that cookies are permanent and that the storage period can be up to two years.

General notes on revocation and objection (so-called "Opt-Out"): Users can revoke the consents they have given at any time and object to the processing in accordance with legal requirements. Users can restrict the use of cookies in their browser settings, among other options (although this may also limit the functionality of our online offering). A objection to the use of cookies for online marketing purposes can also be made through the websites https://optout.aboutads.info and https://www.youronlinechoices.com/.

- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). Consent (Article 6 (1) (a) GDPR).

Further information on processing methods, procedures and services used:

- **Processing Cookie Data on the Basis of Consent:** We use a cookie management solution in which users' consent to the use of cookies, or the procedures and providers mentioned in the cookie management solution, can be obtained, managed and revoked by the users. The declaration of consent is stored so that it does not have to be retrieved again and the consent can be proven in accordance with the legal obligation. Storage can take place server-sided and/or in a cookie (so-called opt-out cookie or with the aid of comparable technologies) in order to be able to assign the consent to a user or and/or his/her device. Subject to individual details of the providers of cookie management services, the following information applies: The duration of the storage of the consent can be up to two years. In this case, a pseudonymous user identifier is formed and stored with the date/time of consent, information on the scope of the consent (e.g. which categories of cookies and/or service providers) as well as the browser, system and used end device; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).

Performing tasks in accordance with statutes or rules of procedure

We process the data of our members, supporters, prospects, business partners or other persons (collectively, " data subjects ") when we have a membership or other business relationship with them and perform our functions and are recipients of benefits and benefits. Otherwise, we process the data of data subjects on the basis of our legitimate interests, e.g. when it concerns administrative tasks or public relations.
The data processed, the type, scope and purpose and the necessity of their processing, are determined by the underlying membership or contractual relationship, from which the necessity of any data information arises (otherwise we refer to necessary data).
We delete data that is no longer required for the performance of our statutory and business purposes. This is determined according to the respective tasks and contractual relationships. We retain the data for as long as it may be relevant for the purpose of conducting business and with regard to any warranty or liability obligations on the basis of our legitimate interest in their regulation. The necessity of storing the data is checked regularly; otherwise the statutory storage obligations apply.

- **Processed data types:** Inventory data (e.g. names, addresses); Payment Data (e.g. bank details, invoices, payment history); Contact data (e.g. e-mail, telephone numbers). Contract data (e.g. contract object, duration, customer category).
- **Data subjects:** Users (e.g. website visitors, users of online services); Members. Business and contractual partners.
- **Purposes of Processing:** Provision of contractual services and fulfillment of contractual obligations; Contact requests and communication. Managing and responding to inquiries.
- **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Provision of online services and web hosting

We process user data in order to be able to provide them with our online services. For this purpose, we process the IP address of the user, which is necessary to transmit the content and functions of our online services to the user's browser or terminal device.

- **Processed data types:** Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Provision of our online services and usability; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.).); Security measures; Web Analytics (e.g. access statistics, recognition of returning visitors); Conversion tracking (Measurement of the effectiveness of marketing activities). Server monitoring and error detection.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Provision of online offer on rented hosting space:** For the provision of our online services, we use storage space, computing capacity and software that we rent or otherwise obtain from a corresponding server provider (also referred to as a "web hoster"); **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- **Collection of Access Data and Log Files:** The access to our online services is logged in the form of so-called "server log files". Server log files may include the address and name of the web pages and files accessed, the date and time of access, data volumes transferred, notification of successful access, browser type and version, the user's operating system, referrer URL (the previously visited page) and, as a general rule, IP addresses and the requesting provider. The server log files can be used for security purposes, e.g. to avoid overloading the servers (especially in the case of abusive attacks, so-called DDoS attacks) and to ensure the stability and optimal load balancing of the servers; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). **Retention period:** Log file information is stored for a maximum period of 30 days and then deleted or anonymized. Data, the further storage of which is necessary for evidence purposes, are excluded from deletion until the respective incident has been finally clarified.
- **Content-Delivery-Network:** We use a so-called "Content Delivery Network" (CDN). A CDN is a service with whose help contents of our online services, in particular large media files, such as graphics or scripts, can be delivered faster

and more securely with the help of regionally distributed servers connected via the Internet; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

- **Squarespace:** Squarespace offers Software as a Service for the creation and hosting of websites; **Service provider**: Squarespace Ireland Ltd., Le Pole House, Ship Street Great, Dublin 8, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.squarespace.com; **Privacy Policy:** https://www.squarespace.com/privacy; **Data Processing Agreement:** https://www.squarespace.com/dpa. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.squarespace.com/dpa).

Blogs and publication media

We use blogs or comparable means of online communication and publication (hereinafter "publication medium"). Readers' data will only be processed for the purposes of the publication medium to the extent necessary for its presentation and communication between authors and readers or for security reasons. For the rest, we refer to the information on the processing of visitors to our publication medium within the scope of this privacy policy.

- **Processed data types:** Inventory data (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Provision of contractual services and fulfillment of contractual obligations; Feedback (e.g. collecting feedback via online form). Provision of our online services and usability.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Contact and Inquiry Management

When contacting us (e.g. via mail, contact form, e-mail, telephone or via social media) as well as in the context of existing user and business relationships, the information of the inquiring persons is processed to the extent necessary to respond to the contact requests and any requested measures.

- **Processed data types:** Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of Processing:** Contact requests and communication; Managing and responding to inquiries; Feedback (e.g. collecting feedback via online form). Provision of our online services and usability.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). Performance of a contract and prior requests (Article 6 (1) (b) GDPR).

Further information on processing methods, procedures and services used:

- **Contact form:** When users contact us via our contact form, e-mail or other communication channels, we process the data provided to us in this context to process the communicated request; **Legal Basis:** Performance of a contract and prior requests (Article 6 (1) (b) GDPR), Legitimate Interests (Article 6 (1) (f) GDPR).

Communication via Messenger

We use messenger services for communication purposes and therefore ask you to observe the following information regarding the functionality of the messenger services, encryption, use of the metadata of the communication and your objection options.
You can also contact us by alternative means, e.g. telephone or e-mail. Please use the contact options provided to you or use the contact options provided within our online services.

In the case of encryption of content (i.e. the content of your message and attachments), we point out that the communication content (i.e. the content of the message and attachments) is encrypted end-to-end. This means that the content of the messages is not visible, not even by the messenger service providers themselves. You should always use a current version of the messenger service with activated encryption, so that the encryption of the message contents is guaranteed.
However, we would like to point out to our communication partners that although messenger service providers do not see the content, they can find out that and when communication partners communicate with us and process technical information on the communication partner's device used and, depending on the settings of their device, also location information (so-called metadata).
Information on Legal basis: If we ask communication partners for permission before communicating with them via messenger services, the legal basis of our processing of their data is their consent. Otherwise, if we do not request consent and you contact us, for example, voluntarily, we use messenger services in our dealings with our contractual partners and as part of the contract initiation process as a contractual measure and in the case of other interested parties and communication partners on the basis of our legitimate interests in fast and efficient communication and meeting the needs of our communication partners for communication via messenger services. We would also like to point out that we do not transmit the contact data provided to us to the messenger service providers for the first time without your consent.
Withdrawal, objection and deletion: You can withdraw your consent or object to communication with us via messenger services at any time. In the case of communication via messenger services, we delete the messages in accordance with our general data retention policy (i.e. as described above after the end of contractual relationships, archiving requirements, etc.) and otherwise as soon as we can assume that we have answered any information provided by the communication partners, if no reference to a previous conversation is to be expected and there are no legal obligations to store the messages to prevent their deletion.
Reservation of reference to other means of communication: Finally, we would like to point out that we reserve the right, for reasons of your safety, not to answer inquiries about messenger services. This is the case if, for example, internal contractual matters require special secrecy or if an answer via the messenger services does not meet

the formal requirements. In such cases we refer you to more appropriate communication channels.

- **Processed data types:** Contact data (e.g. e-mail, telephone numbers); Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status). Content data (e.g. text input, photographs, videos).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of Processing:** Contact requests and communication. Direct marketing (e.g. by e-mail or postal).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Slack:** Instant messaging service; **Service provider**: Slack Technologies, Inc., 500 Howard Street, San Francisco, CA 94105, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://slack.com/; **Privacy Policy:** https://slack.com/intl/en-de/legal; **Data Processing Agreement:** https://slack.com/intl/de-de/terms-of-service/data-processing; **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (https://slack.com/intl/de-de/terms-of-service/data-processing). **Further Information:** Security measures: https://slack.com/intl/en-gb/security-practices.

Video Conferences, Online Meetings, Webinars and Screen-Sharing

We use platforms and applications of other providers (hereinafter referred to as "Conference Platforms") for the purpose of conducting video and audio conferences, webinars and other types of video and audio meetings (hereinafter collectively referred to as "Conference"). When using the Conference Platforms and their services, we comply with the legal requirements.

Data processed by Conference Platforms: In the course of participation in a Conference, the Data of the participants listed below are processed. The scope of the processing depends, on the one hand, on which data is requested in the context of a

specific Conference (e.g., provision of access data or clear names) and which optional information is provided by the participants. In addition to processing for the purpose of conducting the conference, participants' Data may also be processed by the Conference Platforms for security purposes or service optimization. The processed Date includes personal information (first name, last name), contact information (e-mail address, telephone number), access data (access codes or passwords), profile pictures, information on professional position/function, the IP address of the internet access, information on the participants' end devices, their operating system, the browser and its technical and linguistic settings, information on the content-related communication processes, i.e. entries in chats and audio and video data, as well as the use of other available functions (e.g. surveys). The content of communications is encrypted to the extent technically provided by the conference providers. If participants are registered as users with the Conference Platforms, then further data may be processed in accordance with the agreement with the respective Conference Provider.

Logging and recording: If text entries, participation results (e.g. from surveys) as well as video or audio recordings are recorded, this will be transparently communicated to the participants in advance and they will be asked - if necessary - for their consent.

Data protection measures of the participants: Please refer to the data privacy information of the Conference Platforms for details on the processing of your data and select the optimum security and data privacy settings for you within the framework of the settings of the conference platforms. Furthermore, please ensure data and privacy protection in the background of your recording for the duration of a Conference (e.g., by notifying roommates, locking doors, and using the background masking function, if technically possible). Links to the conference rooms as well as access data, should not be passed on to unauthorized third parties.

Notes on legal bases: Insofar as, in addition to the Conference Platforms, we also process users' data and ask users for their consent to use contents from the Conferences or certain functions (e.g. consent to a recording of Conferences), the legal basis of the processing is this consent. Furthermore, our processing may be necessary for the fulfillment of our contractual obligations (e.g. in participant lists, in the case of reprocessing of Conference results, etc.). Otherwise, user data is processed on the basis of our legitimate interests in efficient and secure communication with our communication partners.

- **Processed data types:** Inventory data (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.); Users (e.g. website visitors, users of online services). Persons depicted.
- **Purposes of Processing:** Provision of contractual services and fulfillment of contractual obligations; Contact requests and communication. Office and organisational procedures.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Google Hangouts / Meet:** Conference and communication software; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://hangouts.google.com/; **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:** https://cloud.google.com/terms/data-processing-addendum. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (https://cloud.google.com/terms/eu-model-contract-clause).
- **Microsoft Teams:** Conference and communication software; **Service provider**: Microsoft Irland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.microsoft.com/de-de/microsoft-365; **Privacy Policy:** https://privacy.microsoft.com/de-de/privacystatement, Security information: https://www.microsoft.com/de-de/trustcenter. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA).
- **Slack:** Messenger and conference software; **Service provider**: Slack Technologies Limited, Level 1, Block A Nova Atria North, Sandyford Business District, Dublin 18, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://slack.com/; **Privacy Policy:** https://slack.com/intl/en-

de/legal; **Data Processing Agreement:** https://slack.com/intl/de-de/terms-of-service/data-processing. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (https://slack.com/intl/de-de/terms-of-service/data-processing).

- **Zoom:** Conference and communication software; **Service provider**: Zoom Video Communications, Inc., 55 Almaden Blvd., Suite 600, San Jose, CA 95113, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://zoom.us; **Privacy Policy:** https://zoom.us/docs/de-de/privacy-and-legal.html; **Data Processing Agreement:** https://zoom.us/docs/de-de/privacy-and-legal.html (referred to as Global DPA). **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (https://zoom.us/docs/de-de/privacy-and-legal.html (referred to as Global DPA)).

Job Application Process

The application process requires applicants to provide us with the data necessary for their assessment and selection. The information required can be found in the job description or, in the case of online forms, in the information contained therein.
In principle, the required information includes personal information such as name, address, a contact option and proof of the qualifications required for a particular employment. Upon request, we will be happy to provide you with additional information. If made available, applicants can submit their applications via an online form. The data will be transmitted to us encrypted according to the state of the art. Applicants can also send us their applications by e-mail. Please note, however, that e-mails on the Internet are generally not sent in encrypted form. As a rule, e-mails are encrypted during transport, but not on the servers from which they are sent and received. We can therefore accept no responsibility for the transmission path of the application between the sender and the reception on our server. For the purposes of searching for applicants, submitting applications and selecting applicants, we may make use of the applicant management and recruitment software, platforms and services of third-party providers in compliance with legal requirements. Applicants are welcome to contact us about how to submit their application or send it to us by regular mail.

Processing of special categories of data: To the extent that special categories of personal data (Article 9(1) GDPR, e.g., health data, such as disability status or ethnic origin) are requested from applicants or communicated by them during the application process, their processing is carried out so that the controller or the data subject can exercise rights arising from employment law and the law of social security and social protection, in the case of protection of vital interests of the applicants or other persons, or for purposes of preventive or occupational medicine, for the assessment of the employee's work ability, for medical diagnosis, for the provision or treatment in the health or social sector, or for the management of systems and services in the health or social sector.

Ereasure of data: In the event of a successful application, the data provided by the applicants may be further processed by us for the purposes of the employment relationship. Otherwise, if the application for a job offer is not successful, the applicant's data will be deleted. Applicants' data will also be deleted if an application is withdrawn, to which applicants are entitled at any time. Subject to a justified revocation by the applicant, the deletion will take place at the latest after the expiry of a period of six months, so that we can answer any follow-up questions regarding the application and comply with our duty of proof under the regulations on equal treatment of applicants. Invoices for any reimbursement of travel expenses are archived in accordance with tax regulations.

Admission to a talent pool - Admission to a talent pool, if offered, is based on consent. Applicants are informed that their consent to be included in the talent pool is voluntary, has no influence on the current application process and that they can revoke their consent at any time for the future.

- **Processed data types:** Inventory data (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos). Job applicant details (e.g. Personal data, postal and contact addresses and the documents pertaining to the application and the information contained therein, such as cover letter, curriculum vitae, certificates, etc., as well as other information on the person or qualifications of applicants provided with regard to a specific job or voluntarily by applicants).
- **Data subjects:** Job applicants.

- **Purposes of Processing:** Job Application Process (Establishment and possible later execution as well as possible later termination of the employment relationship).
- **Legal Basis:** Job application process as a pre-contractual or contractual relationship (Article 6 (1) (b) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **LinkedIn Recruiter:** Job search and application related services within the LinkedIn platform; **Service provider**: LinkedIn Ireland Unlimited Company, Wilton Plaza Wilton Place, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.linkedin.com; **Terms & Conditions:** https://legal.linkedin.com/dpa; **Privacy Policy:** https://www.linkedin.com/legal/privacy-policy; **Data Processing Agreement:** https://legal.linkedin.com/dpa. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF).
- **myInterview:** Video recruiting platform; **Service provider**: myInterview Ltd.
  Hagag Tower
  156 Menachem Begin
  Tel Aviv 6492108
  Israel
  ; **Website:** https://myinterview.com. **Privacy Policy:** https://myinterview.com/privacy#privacy.

Cloud Services

We use Internet-accessible software services (so-called "cloud services", also referred to as "Software as a Service") provided on the servers of its providers for the storage and management of content (e.g. document storage and management, exchange of documents, content and information with certain recipients or publication of content and information).
Within this framework, personal data may be processed and stored on the provider's servers insofar as this data is part of communication processes with us or is otherwise processed by us in accordance with this privacy policy. This data may include in

particular master data and contact data of data subjects, data on processes, contracts, other proceedings and their contents. Cloud service providers also process usage data and metadata that they use for security and service optimization purposes.
If we use cloud services to provide documents and content to other users or publicly accessible websites, forms, etc., providers may store cookies on users' devices for web analysis or to remember user settings (e.g. in the case of media control).

- **Processed data types:** Inventory data (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status). Images and/ or video recordings (e.g. photographs or video recordings of a person).
- **Data subjects:** Customers; Employees (e.g. Employees, job applicants); Prospective customers; Communication partner (Recipients of e-mails, letters, etc.). Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Office and organisational procedures; Information technology infrastructure (Operation and provision of information systems and technical devices, such as computers, servers, etc.).). Provision of contractual services and fulfillment of contractual obligations.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Adobe Creative Cloud:** Cloud storage, cloud infrastructure services, and cloud-based application software, among others for photo editing, video editing, graphic design, web development; **Service provider**: Adobe Systems Software Ireland, 4-6, Riverwalk Drive, Citywest Business Campus, Brownsbarn, Dublin 24, D24 DCW0, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.adobe.com/creativecloud.html; **Privacy Policy:** https://www.adobe.com/privacy.html; **Data Processing Agreement:** Provided by the service provider. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider).
- **Google Workspace:** Cloud storage, cloud infrastructure services and cloud-based application software; **Service provider**: Google Cloud EMEA Limited, 70 Sir John Rogerson’s Quay, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests

(Article 6 (1) (f) GDPR); **Website:** https://workspace.google.com/; **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:** https://cloud.google.com/terms/data-processing-addendum; **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (https://cloud.google.com/terms/eu-model-contract-clause). **Further Information:** https://cloud.google.com/privacy.

- **Microsoft Cloud Services:** Cloud storage, cloud infrastructure services and cloud-based application software; **Service provider**: Microsoft Irland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://microsoft.com; **Privacy Policy:** https://privacy.microsoft.com/de-de/privacystatement, Security information: https://www.microsoft.com/de-de/trustcenter; **Data Processing Agreement:** https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA).

Newsletter and Electronic Communications

We send newsletters, e-mails and other electronic communications (hereinafter referred to as "newsletters") only with the consent of the recipient or a legal permission. Insofar as the contents of the newsletter are specifically described within the framework of registration, they are decisive for the consent of the user. Otherwise, our newsletters contain information about our services and us.

In order to subscribe to our newsletters, it is generally sufficient to enter your e-mail address. We may, however, ask you to provide a name for the purpose of contacting you personally in the newsletter or to provide further information if this is required for the purposes of the newsletter.

Double opt-in procedure: The registration to our newsletter takes place in general in a so-called Double-Opt-In procedure. This means that you will receive an e-mail after

registration asking you to confirm your registration. This confirmation is necessary so that no one can register with external e-mail addresses.
The registrations for the newsletter are logged in order to be able to prove the registration process according to the legal requirements. This includes storing the login and confirmation times as well as the IP address. Likewise the changes of your data stored with the dispatch service provider are logged.
Deletion and restriction of processing: We may store the unsubscribed email addresses for up to three years based on our legitimate interests before deleting them to provide evidence of prior consent. The processing of these data is limited to the purpose of a possible defense against claims. An individual deletion request is possible at any time, provided that the former existence of a consent is confirmed at the same time. In the case of an obligation to permanently observe an objection, we reserve the right to store the e-mail address solely for this purpose in a blocklist.
The logging of the registration process takes place on the basis of our legitimate interests for the purpose of proving its proper course. If we commission a service provider to send e-mails, this is done on the basis of our legitimate interests in an efficient and secure sending system.
Contents:

Information about us, our services, promotions and offers.

- **Processed data types:** Inventory data (e.g. names, addresses); Contact data (e.g. e-mail, telephone numbers); Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status). Usage data (e.g. websites visited, interest in content, access times).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of Processing:** Direct marketing (e.g. by e-mail or postal).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).
- **Opt-Out:** You can cancel the receipt of our newsletter at any time, i.e. revoke your consent or object to further receipt. You will find a link to cancel the newsletter either at the end of each newsletter or you can otherwise use one of the contact options listed above, preferably e-mail.

Further information on processing methods, procedures and services used:

- **Measurement of opening rates and click rates:** The newsletters contain a so-called "web-beacon", i.e. a pixel-sized file, which is retrieved from our server when the newsletter is opened or, if we use a mailing service provider, from its server. Within the scope of this retrieval, technical information such as information about the browser and your system, as well as your IP address and time of retrieval are first collected.

  This information is used for the technical improvement of our newsletter on the basis of technical data or target groups and their reading behaviour on the basis of their retrieval points (which can be determined with the help of the IP address) or access times. This analysis also includes determining whether newsletters are opened, when they are opened and which links are clicked. This information is assigned to the individual newsletter recipients and stored in their profiles until the profiles are deleted. The evaluations serve us much more to recognize the reading habits of our users and to adapt our content to them or to send different content according to the interests of our users.

  The measurement of opening rates and click rates as well as the storage of the measurement results in the profiles of the users and their further processing are based on the consent of the users.

  A separate objection to the performance measurement is unfortunately not possible, in this case the entire newsletter subscription must be cancelled or objected to. In this case, the stored profile information will be deleted; **Legal Basis:** Consent (Article 6 (1) (a) GDPR).
- **Mailchimp:** Email distribution and email marketing platform; **Service provider**: Rocket Science Group, LLC, 675 Ponce De Leon Ave NE #5000, Atlanta, GA 30308, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://mailchimp.com; **Privacy Policy:** https://mailchimp.com/legal/; **Data Processing Agreement:** https://mailchimp.com/legal/data-processing-addendum/; **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (Provided by the service provider). **Further Information:** Special

safety measures: https://mailchimp.com/help/Mailchimp-european-data-transfers/.

Commercial communication by E-Mail, Postal Mail, Fax or Telephone

We process personal data for the purposes of promotional communication, which may be carried out via various channels, such as e-mail, telephone, post or fax, in accordance with the legal requirements.
The recipients have the right to withdraw their consent at any time or to object to the advertising communication at any time.
After revocation or objection, we store the data required to prove the past authorization to contact or send up to three years from the end of the year of revocation or objection on the basis of our legitimate interests. The processing of this data is limited to the purpose of a possible defense against claims. Based on the legitimate interest to permanently observe the revocation, respectively objection of the users, we further store the data necessary to avoid a renewed contact (e.g. depending on the communication channel, the e-mail address, telephone number, name).

- **Processed data types:** Inventory data (e.g. names, addresses). Contact data (e.g. e-mail, telephone numbers).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.).
- **Purposes of Processing:** Direct marketing (e.g. by e-mail or postal).
- **Legal Basis:** Consent (Article 6 (1) (a) GDPR). Legitimate Interests (Article 6 (1) (f) GDPR).

Surveys and Questionnaires

We conduct surveys and interviews to gather information for the survey purpose communicated in each case. The surveys and questionnaires ("surveys") carried out by us are evaluated anonymously. Personal data is only processed insofar as this is necessary for the provision and technical execution of the survey (e.g. processing the IP address to display the survey in the user's browser or to enable a resumption of the survey with the aid of a cookie).

- **Processed data types:** Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.). Participants.
- **Purposes of Processing:** Feedback (e.g. collecting feedback via online form).
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Google Forms:** Creation and evaluation of online forms, surveys, feedback forms, etc; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.google.de/intl/en/forms/about/; **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:** https://cloud.google.com/terms/data-processing-addendum. **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (https://cloud.google.com/terms/eu-model-contract-clause).

Web Analysis, Monitoring and Optimization

Web analysis is used to evaluate the visitor traffic on our website and may include the behaviour, interests or demographic information of users, such as age or gender, as pseudonymous values. With the help of web analysis we can e.g. recognize, at which time our online services or their functions or contents are most frequently used or requested for repeatedly, as well as which areas require optimization.
In addition to web analysis, we can also use test procedures, e.g. to test and optimize different versions of our online services or their components.
Unless otherwise stated below, profiles, i.e. data aggregated for a usage process, can be created for these purposes and information can be stored in a browser or in a terminal device and read from it. The information collected includes, in particular, websites visited and elements used there as well as technical information such as the browser used, the computer system used and information on usage times. If users have agreed to the

collection of their location data from us or from the providers of the services we use, location data may also be processed.
Unless otherwise stated below, profiles, that is data summarized for a usage process or user, may be created for these purposes and stored in a browser or terminal device (so-called "cookies") or similar processes may be used for the same purpose. The information collected includes, in particular, websites visited and elements used there as well as technical information such as the browser used, the computer system used and information on usage times. If users have consented to the collection of their location data or profiles to us or to the providers of the services we use, these may also be processed, depending on the provider.
The IP addresses of the users are also stored. However, we use any existing IP masking procedure (i.e. pseudonymisation by shortening the IP address) to protect the user. In general, within the framework of web analysis, A/B testing and optimisation, no user data (such as e-mail addresses or names) is stored, but pseudonyms. This means that we, as well as the providers of the software used, do not know the actual identity of the users, but only the information stored in their profiles for the purposes of the respective processes.

- **Processed data types:** Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Web Analytics (e.g. access statistics, recognition of returning visitors). Profiles with user-related information (Creating user profiles).
- **Security measures:** IP Masking (Pseudonymization of the IP address).

Profiles in Social Networks (Social Media)

We maintain online presences within social networks and process user data in this context in order to communicate with the users active there or to offer information about us.
We would like to point out that user data may be processed outside the European Union. This may entail risks for users, e.g. by making it more difficult to enforce users' rights.

In addition, user data is usually processed within social networks for market research and advertising purposes. For example, user profiles can be created on the basis of user behaviour and the associated interests of users. The user profiles can then be used, for example, to place advertisements within and outside the networks which are presumed to correspond to the interests of the users. For these purposes, cookies are usually stored on the user's computer, in which the user's usage behaviour and interests are stored. Furthermore, data can be stored in the user profiles independently of the devices used by the users (especially if the users are members of the respective networks or will become members later on).
For a detailed description of the respective processing operations and the opt-out options, please refer to the respective data protection declarations and information provided by the providers of the respective networks.
Also in the case of requests for information and the exercise of rights of data subjects, we point out that these can be most effectively pursued with the providers. Only the providers have access to the data of the users and can directly take appropriate measures and provide information. If you still need help, please do not hesitate to contact us.

- **Processed data types:** Contact data (e.g. e-mail, telephone numbers); Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Contact requests and communication; Feedback (e.g. collecting feedback via online form). Marketing.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **LinkedIn:** Social network; **Service provider**: LinkedIn Ireland Unlimited Company, Wilton Plaza Wilton Place, Dublin 2, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.linkedin.com; **Privacy Policy:** https://www.linkedin.com/legal/privacy-policy; **Basis for third country transfer:** EU-US Data Privacy Framework (DPF), Standard Contractual Clauses (https://legal.linkedin.com/dpa); **Opt-Out:** https://www.linkedin.com/psettings/guest-controls/retargeting-opt-out. **Further**

Information: We are jointly responsible with LinkedIn Ireland Unlimited Company for the collection (but not the further processing) of data from visitors for the purposes of creating Page Insights for our LinkedIn profiles. This data includes information about the types of content that users view or interact with, or the actions they take, as well as information about the devices used by the users (e.g., IP addresses, operating system, browser type, language settings, cookie data) and details from the users' profiles, such as job function, country, industry, seniority, company size, and employment status. Privacy information regarding the processing of user data by LinkedIn can be found in LinkedIn's privacy notices: https://www.linkedin.com/legal/privacy-policy
We have concluded a special agreement with LinkedIn Irland, the 'Page Insights Joint Controller Addendum (the 'Addendum')' (https://legal.linkedin.com/pages-joint-controller-addendum), which specifically regulates the security measures that LinkedIn must observe and wherein LinkedIn has agreed to fulfill the rights of the affected parties (i.e., users can, for example, direct requests for information or deletion directly to LinkedIn). The rights of the users (in particular to access to information, erasure, objection, and complaint to the competent supervisory authority) are not restricted by the agreements with LinkedIn. The joint responsibility is limited to the collection of data by and transmission to Ireland Unlimited Company, a company based in the EU. The further processing of the data is the sole responsibility of Ireland Unlimited Company, particularly regarding the transmission of data to the parent company LinkedIn Corporation in the USA.

- **X:** Social network; **Service provider**: Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2 D02 AX07, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR). **Privacy Policy:** https://twitter.com/privacy, (Settings: https://twitter.com/personalization).

Plugins and embedded functions and content

Within our online services, we integrate functional and content elements that are obtained from the servers of their respective providers (hereinafter referred to as "third-

party providers"). These may, for example, be graphics, videos or city maps (hereinafter uniformly referred to as "Content").
The integration always presupposes that the third-party providers of this content process the IP address of the user, since they could not send the content to their browser without the IP address. The IP address is therefore required for the presentation of these contents or functions. We strive to use only those contents, whose respective offerers use the IP address only for the distribution of the contents. Third parties may also use so-called pixel tags (invisible graphics, also known as "web beacons") for statistical or marketing purposes. The "pixel tags" can be used to evaluate information such as visitor traffic on the pages of this website. The pseudonymous information may also be stored in cookies on the user's device and may include technical information about the browser and operating system, referring websites, visit times and other information about the use of our website, as well as may be linked to such information from other sources.

- **Processed data types:** Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Provision of our online services and usability.
- **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).

Further information on processing methods, procedures and services used:

- **Google Fonts (from Google Server):** Obtaining fonts (and symbols) for the purpose of a technically secure, maintenance-free and efficient use of fonts and symbols with regard to timeliness and loading times, their uniform presentation and consideration of possible restrictions under licensing law. The provider of the fonts is informed of the user's IP address so that the fonts can be made available in the user's browser. In addition, technical data (language settings, screen resolution, operating system, hardware used) are transmitted which are necessary for the provision of the fonts depending on the devices used and the technical environment. This data may be processed on a server of the provider of the fonts in the USA - When visiting our online services, users' browsers send their browser HTTP requests to the Google Fonts Web API. The Google Fonts Web API provides users with Google Fonts' cascading style sheets (CSS) and then with the fonts specified in the CCS. These HTTP requests include (1) the IP address used by each user to access the Internet, (2) the requested URL on the

Google server, and (3) the HTTP headers, including the user agent describing the browser and operating system versions of the website visitors, as well as the referral URL (i.e., the web page where the Google font is to be displayed). IP addresses are not logged or stored on Google servers and they are not analyzed. The Google Fonts Web API logs details of HTTP requests (requested URL, user agent, and referring URL). Access to this data is restricted and strictly controlled. The requested URL identifies the font families for which the user wants to load fonts. This data is logged so that Google can determine how often a particular font family is requested. With the Google Fonts Web API, the user agent must match the font that is generated for the particular browser type. The user agent is logged primarily for debugging purposes and is used to generate aggregate usage statistics that measure the popularity of font families. These aggregate usage statistics are published on Google Fonts' Analytics page. Finally, the referral URL is logged so that the data can be used for production maintenance and to generate an aggregate report on top integrations based on the number of font requests. Google says it does not use any of the information collected by Google Fonts to profile end users or serve targeted ads; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://fonts.google.com/; **Privacy Policy:** https://policies.google.com/privacy; **Basis for third country transfer:** EU-US Data Privacy Framework (DPF). **Further Information:** https://developers.google.com/fonts/faq/privacy?hl=en.

Management, Organization and Utilities

We use services, platforms and software from other providers (hereinafter referred to as " third-party providers") for the purposes of organizing, administering, planning and providing our services. When selecting third-party providers and their services, we comply with the legal requirements.
Within this context, personal data may be processed and stored on the servers of third-party providers. This may include various data that we process in accordance with this privacy policy. This data may include in particular master data and contact data of users, data on processes, contracts, other processes and their contents.

If users are referred to the third-party providers or their software or platforms in the context of communication, business or other relationships with us, the third-party provider processing may process usage data and metadata that can be processed by them for security purposes, service optimisation or marketing purposes. We therefore ask you to read the data protection notices of the respective third party providers.

- **Processed data types:** Content data (e.g. text input, photographs, videos); Usage data (e.g. websites visited, interest in content, access times). Meta, communication and process data (e.g. IP addresses, time information, identification numbers, consent status).
- **Data subjects:** Communication partner (Recipients of e-mails, letters, etc.). Users (e.g. website visitors, users of online services).
- **Purposes of Processing:** Provision of contractual services and fulfillment of contractual obligations. Office and organisational procedures.