Privacy policy (as of 2026/20/10)

We at Platform Control take the protection of your data very seriously. To this end, we limit data processing to the absolute minimum. At the same time, with this "10 out of 10 Privacy Policy", we want to explain to you in a comprehensible, transparent and understandable way how your personal data is processed and how we comply with the requirements of the EU General Data Protection Regulation (GDPR) (**"GDPR"**), the Federal Data Protection Act (**"BDSG"**) and the Telecommunications Digital Services Data Protection Act (**„TDDDG"**) on our website and in the event that you submit a case to us. 10 out of 10? Instead of lengthy and incomprehensible privacy policies, we present you with ten essential questions on ten pages.

Privacy Policy

- 1. Who is the responsible contact person?
- 2. What data do you collect when processing cases?
- 3. What happens to my data during case processing?
- 4. What security measures do you take?
- 5. Is data processed in third countries?
- 6. When will my data be deleted?
- 7. What are my rights as an affected person?
- 8. What data is processed when visiting the website and through the provision of the online service and web hosting?
- 9. And what about cookies?
- 10. How is data processed within the context of contact and inquiry management?

1. Who is the responsible contact person?

Platform Control GmbH
Lochhamer Straße 18
82166 Gräfelfing

Authorized representatives: Managing Director Dr. David Korb, Maximilian Nerlich
Privacy Officer: Julius Nerlich
Email Address: info@platform-control.com
Imprint: https://platform-control.com/impressum/

2. What data do you collect when processing cases?

If you decide to file a complaint, you will be asked to provide us with the following personal data, among other things:

- Personal data such as name, place of residence, nationality, location, email address & telephone number;
- Moderation decision of the online platform
- Content data of the content itself and, if applicable, a link;
- Platform case ID, if one has been assigned;
- Your statement of facts
- Evidence and other documents provided.

This data is absolutely essential for processing your case. We do not collect any additional data that is not required for this case. By submitting a complaint, this data is stored and therefore already processed by us. No data beyond the information you provide will be processed in relation to your case. You therefore have complete control over the data we process in connection with your case.

The data from submitted cases will be processed and stored exclusively on GDPR-compliant infrastructure provided by Akenes SA, Boulevard de Grancy 19A, 1006 Lausanne, Switzerland (Exoscale), specifically in Exoscale's German data centers in Frankfurt am Main and Munich. The Frankfurt data center is certified according to ISO 9001, 14001, 27001, and 50001. It is also certified according to PCI DSS 3.2 and OHSAS 18001. The Munich data center is certified according to ISO 9001 and 27001, as well as PCI DSS 3.2, SoC Type II, and SOC-2 Type II. More information about Exoscale's data centers can be found at https://www.exoscale.com/datacenters/.

3. What happens to my data during case processing?

To decide your case, we require a statement from the online platform. For this purpose, it is necessary to forward the information you provided to the online platform. Your data will be processed by us or our employees, who process the data under our supervision only for the intended purpose pursuant to Art. 29 GDPR.

As soon as the online platform has responded to us (or the deadline has expired without result), the data of your case, which is now ready for a decision, will be processed by us, our employees, and, if applicable, external case decision-makers as part of drafting a decision. The data is processed using word processing programs and cloud services provided by the processor Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, Email: support-deutschland@google.com. Data processing agreements pursuant to Art. 28 GDPR ensure the security of your data during the case decision process. In principle, anyone who comes into contact with the case data is obligated to comply with applicable data protection laws. Our Data Protection Officer ensures compliance.

The processing by our data processors ends when the decision is delivered to you and the online platform via email. Further processing is limited to storing your data on the relevant servers (for deletion see question 6).

Your personal data will not be included in the “Transparency Reports” that we are required to submit to the Federal Network Agency as Germany’s Digital Service Coordinator. These reports only provide abstract figures without any connection to individual users (e.g., X complaints in December 2025, average processing time of XY days, etc.).

4. What security measures do you take?

In accordance with 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 varying likelihood and severity of the threat to the rights and freedoms of natural persons, we implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

These measures include, in particular, the signing of comprehensive data processing agreements pursuant to Article 28 GDPR, which provide information on compliance with the regulations. Furthermore, all individuals exposed to personal data are required to sign codes of conduct, which explicitly address the confidentiality, integrity, and availability of data by controlling physical and electronic access to the data, as well as access to, input of, transfer of, and ensuring the availability and segregation of the data. We have also established procedures that guarantee the exercise of data subject rights, the deletion of data, and responses to data breaches. Moreover, we consider the protection of personal data during the development and selection of hardware, software, and processes, in accordance with the principles of data protection by design and by default, and especially by collecting only the data necessary for carrying out the process.

IP address truncation: If IP addresses are processed by us or by the service providers and technologies we use, and processing a full IP address is not necessary, the IP address is truncated (also known as "IP masking"). This involves removing the last two digits, or the last part of the IP address after a period, or replacing them with placeholders. The purpose of truncating the IP address is to prevent or significantly hinder the identification of a person based on their IP address.

Securing online connections with TLS/SSL encryption technology (HTTPS): To protect user data transmitted through our online services from unauthorized access, we rely on TLS/SSL encryption technology. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are the cornerstones of secure data transmission on the internet. These technologies encrypt the information transmitted between the website or app and the user's browser (or between two servers), thus protecting the data from unauthorized access. TLS, as the more advanced and secure version of SSL, ensures that all data transmissions meet the highest security standards. When a website is secured with an SSL/TLS certificate, this is indicated by the display of HTTPS in the URL. This serves as an indicator to users that their data is being transmitted securely and encrypted.

5. Is data processed in third countries?

Mostly no. Our servers are located in Germany, see question 3. Direct processing in third countries would not comply with the GDPR. Accordingly, the data processing agreements do not permit processing in third countries.

However, the data will be forwarded to the online platform for obtaining a statement, which may be located outside the EU. In this case, processing by the online platform takes place in a third country. If we transfer data to a third country (i.e., outside the European Union (EU) or the European Economic Area (EEA)), or if this occurs in the context of using third-party services or disclosing or transferring data to other persons, entities, or companies (which is

identifiable by the postal address of the respective provider or if the privacy policy explicitly refers to the data transfer to third countries), this is always done in accordance with legal requirements.

For data transfers to the USA, we primarily rely on the Data Privacy Framework (DPF), which was recognized as a secure legal framework by an adequacy decision of the EU Commission on July 10, 2023. In addition, we have concluded standard contractual clauses with the respective providers, which comply with the requirements of the EU Commission and establish contractual obligations for the protection of your data.

This dual safeguard ensures comprehensive protection of your data: The Data Protection Framework (DPF) forms the primary layer of protection, while the Standard Contractual Clauses serve as an additional safeguard. Should changes occur within the framework of the DPF, the Standard Contractual Clauses act as a reliable fallback option. This ensures that your data remains adequately protected even in the event of any political or legal changes.

For each service provider, we will inform you whether they are DPF-certified and whether standard contractual clauses are in place. Further information about the DPF and a list of certified companies can be found on the U.S. Department of Commerce website at [website address]. https://www.dataprivacyframework.gov/(in English).

For data transfers to other third countries, appropriate safeguards apply, in particular standard contractual clauses, explicit consent, or legally required transfers. You can find information on third-country transfers and applicable adequacy decisions in the EU Commission's information resources: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en?prefLang=de.

6. When will my data be deleted?

We delete personal data that we process in accordance with legal regulations as soon as the underlying consents are withdrawn or no further legal basis for processing exists. This applies to cases where the original processing purpose no longer applies or the data is no longer needed. Exceptions to this rule exist if legal obligations or special interests require longer retention or archiving of the data.

Data that must be retained for commercial or tax law reasons, or whose storage is necessary for legal proceedings or to protect the rights of other natural or legal persons, will be archived accordingly. Our privacy policy contains additional information on data retention and deletion that applies specifically to certain processing activities.

If there are multiple specifications regarding the retention period or deletion deadlines for a given date, the longest period always applies.

If a time limit does not expressly begin on a specific date and is at least one year, it starts automatically at the end of the calendar year in which the event triggering the time limit occurred. In the case of ongoing contractual relationships in which data is stored, the event triggering the time limit is the effective date of the termination or other end of the legal relationship.

Data that is no longer retained for the originally intended purpose, but is retained due to legal requirements or other reasons, is processed by us exclusively for the reasons that justify its retention.

Further information on processing procedures, methods and services:

- **Data storage and deletion:** The following general retention periods apply under German law for storage and archiving:
    - 10 years - Retention period for books and records, annual financial statements, inventories, management reports, opening balance sheets and the work instructions and other organizational documents required for their understanding (§ 147 para. 1 no. 1 in conjunction with para. 3 AO, § 14b para. 1 UStG, § 257 para. 1 no. 1 in conjunction with para. 4 HGB).
    - 8 years - accounting documents, such as invoices and cost receipts (§ 147 para. 1 no. 4 and 4a in conjunction with para. 3 sentence 1 AO as well as § 257 para. 1 no. 4 in conjunction with para. 4 HGB).
    - 6 years - Other business documents: received commercial or business letters, copies of sent commercial or business letters, other documents insofar as they are relevant for taxation, e.g. timesheets, operating statements, costing documents, price labels, but also payroll documents, insofar as they are not already accounting documents and cash register tapes (§ 147 para. 1 no. 2, 3, 5 in conjunction with para. 3 AO, § 257 para. 1 no. 2 and 3 in conjunction with para. 4 HGB).
    - 3 years - Data required to consider potential warranty and damage claims or similar contractual claims and rights, as well as to process related inquiries, based on previous business experience and standard industry practices, will be stored for the duration of the regular statutory limitation period of three years (§§ 195, 199 BGB).

7. What are my rights as an affected person?

Rights of data subjects under the GDPR: As a data subject, you have various rights under the GDPR, which arise in particular from Articles 15 to 21 GDPR:

- Right to object: You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you which is based on point (e) or (f) of Article 6(1) of the GDPR, including profiling based on those provisions. Where personal data concerning you are processed for direct marketing purposes, you have the right to object at any time to processing of personal data concerning you for such marketing, which includes profiling to the extent that it is related to such direct marketing.
- **Right of withdrawal for consents:**You have the right to withdraw your consent at any time.
- **Right to information:**You have the right to request confirmation as to whether your personal data is being processed, and to access this data as well as further information and a copy of the data in accordance with legal requirements.
- **Right to rectification:**In accordance with legal requirements, you have the right to request the completion of data concerning you or the correction of inaccurate data concerning you.

- **Right to erasure and restriction of processing:**In accordance with legal requirements, you have the right to request that data concerning you be deleted immediately, or alternatively, in accordance with legal requirements, to request a restriction of the processing of the data.
- **Right to data portability:**You have the right to receive the data concerning you that you have provided to us in a structured, commonly used and machine-readable format, in accordance with the legal requirements, or to request its transmission to another controller.
- **Complaint to the supervisory authority:**Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, your place of work or the place of the alleged infringement, if you consider that the processing of personal data relating to you infringes the GDPR.

8. What data is processed when visiting the website and through the provision of the online service and web hosting?

For our website to function, certain data, such as your IP address, must be transmitted to us. Without this, websites would not be displayed correctly. When you visit our website, the following data is collected for technical reasons to enable its functionality. Some of this data is personal data. This data is then stored briefly in a server log file:

Data types processed: Usage data (e.g., page views and time spent on the site, click paths, usage intensity and frequency, device types and operating systems used, interactions with content and functions); metadata, communication data, and procedural data (e.g., IP addresses, timestamps, identification numbers, individuals involved); log data (e.g., log files concerning logins or data retrieval or access times); content data (e.g., textual or image-based messages and posts, as well as related information such as authorship or creation date).

- **Affected persons:** Users (e.g., website visitors, users of online services).
- **Purposes of processing:** Provision of our online services and user-friendliness; information technology infrastructure (operation and provision of information systems and technical equipment (computers, servers, etc.)). Security measures.
- **Storage and deletion:** Deletion according to the information in the section "General information on data storage and deletion".
- **Legal basis:** Legitimate interests (Art. 6 para. 1 sentence 1 lit. f) GDPR).

Further information on processing procedures, methods and services:

- **Provision of online services on rented storage space:** To provide our online services, we use storage space, computing capacity and software that we rent from a corresponding server provider (also called "web host") or obtain from other sources; **Legal basis:** Legitimate interests (Art. 6 para. 1 sentence 1 lit. f) GDPR).
- **Collection of access data and log files:** Access to our online services is logged in the form of so-called "server log files." These server log files may contain the address and name of the accessed web pages and files, the date and time of access, the amount of data transferred, notification of successful access, browser type and version, the user's operating system, referrer URL (the previously visited page), and,

typically, IP addresses and the requesting provider. Server log files can be used for security purposes, such as preventing server overload (especially in the case of malicious attacks, so-called DDoS attacks), and to ensure server capacity and stability. **Legal basis:** Legitimate interests (Art. 6 para. 1 sentence 1 lit. f) GDPR). **Deletion of data:** Log file information is stored for a maximum of 30 days and then deleted or anonymized. Data that needs to be retained for evidentiary purposes is exempt from deletion until the respective incident has been fully resolved.

- **Email sending and hosting:** The web hosting services we use also include sending, receiving, and storing emails. For these purposes, the addresses of the recipients and senders, as well as other information relating to email transmission (e.g., the providers involved) and the content of the respective emails, are processed. The aforementioned data may also be processed for spam detection purposes. Please note that emails are generally not encrypted when sent over the internet. While emails are usually encrypted during transmission, they are not encrypted on the servers from which they are sent and received (unless end-to-end encryption is used). Therefore, we cannot assume any responsibility for the transmission of emails between the sender and their arrival on our server. **Legal basis:** Legitimate interests (Art. 6 para. 1 sentence 1 lit. f) GDPR).
- **ALL-INCLUSIVE:** Services in the field of providing information technology infrastructure and related services (e.g. storage space and/or computing capacity); **Service provider:** ALL-INKL.COM - Neue Medien Münnich, Owner: René Münnich, Hauptstraße 68, 02742 Friedersdorf, Germany; **Legal basis:**Legitimate interests (Art. 6 para. 1 sentence 1 lit. f) GDPR); **Website:** https://all-inkl.com/; **Privacy Policy:** https://all-inkl.com/datenschutzinformationen/. **Data processing agreement:** Provided by the service provider.

9. And what about cookies?

The term "cookies" refers to functions that store information on and read it from users' devices. Cookies can also be used for various purposes, such as ensuring the functionality, security, and user-friendliness of online services, as well as analyzing visitor traffic. We use cookies in accordance with legal regulations. Where necessary, we obtain users' consent beforehand. If consent is not required, we rely on our legitimate interests. This applies when storing and reading information is essential to providing explicitly requested content and functions. This includes, for example, saving settings and ensuring the functionality and security of our online services. Consent can be withdrawn at any time. We provide clear information about the scope of this consent and which cookies are used.

Information on the legal basis for data protection: Whether we process personal data using cookies depends on consent. If consent has been given, it serves as the legal basis. Without consent, we rely on our legitimate interests, which are explained above in this section and in the context of the respective services and procedures.

Storage duration: With regard to storage duration, the following types of cookies are distinguished:

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

- **Permanent Cookies:** Persistent cookies remain stored even after the device is closed. This allows, for example, login status to be saved and preferred content to be displayed directly when the user revisits a website. Similarly, user data collected using cookies can be used for audience measurement. Unless we explicitly inform users about the type and storage duration of cookies (e.g., when obtaining consent), you should assume that these cookies are persistent and can be stored for up to two years.

General information on revocation and objection (opt-out): Users can revoke their consent at any time and also object to the processing in accordance with legal requirements, including via their browser's privacy settings.

- **Data types processed:** Metadata, communication data and process data (e.g. IP addresses, timestamps, identification numbers, persons involved).
- **Affected persons:** Users (e.g., website visitors, users of online services).
- **Legal basis:** Legitimate interests (Art. 6 para. 1 sentence 1 lit. f) GDPR). Consent (Art. 6 para. 1 sentence 1 lit. a) GDPR).

Further information on processing procedures, methods and services:

- **Processing of cookie data based on consent:** We use a consent management solution to obtain user consent for the use of cookies or for the processes and providers mentioned within the consent management solution. This process serves to obtain, log, manage, and revoke consent, particularly regarding the use of cookies and similar technologies that are used to store, read, and process information on users' devices. Within this process, user consent for the use of cookies and the associated processing of information, including the specific processing activities and providers mentioned in the consent management process, is obtained. Users also have the option to manage and revoke their consent. The declarations of consent are stored to avoid repeated requests and to provide proof of consent in accordance with legal requirements. Storage takes place server-side and/or in a cookie (so-called opt-in cookie) or using comparable technologies to assign the consent to a specific user or their device. Unless specific information is available regarding the providers of consent management services, the following general guidelines apply: Consent is stored for up to two years. A pseudonymous user identifier is created, which is stored together with the time of consent, details of the scope of consent (e.g., categories of cookies and/or service providers concerned), and information about the browser, system, and device used.**Legal basis:**Consent (Art. 6 para. 1 sentence 1 lit. a) GDPR).
- **Complianz:** Consent management: Procedures for obtaining, logging, managing and withdrawing consent, in particular for the use of cookies and similar technologies for storing, reading and processing information on users' end devices and their processing;**Service provider:**Execution on servers and/or computers under own data protection responsibility;**Website:** https://complianz.io/; **Privacy Policy:** https://complianz.io/legal/. **Further information:**An individual user ID, language, types of consent and the time of their submission are stored server-side and in the cookie on the user's device.

10. How is data processed within the context of contact and inquiry management?

When you contact us (e.g. by mail, contact form, email, telephone or via social media) and within the framework of existing user and business relationships, the information provided by the requesting persons is processed to the extent necessary to answer the contact requests and any requested measures.

- **Data types processed:** Inventory data (e.g., full name, home address, contact information, customer number, etc.); contact data (e.g., postal and email addresses or telephone numbers); content data (e.g., textual or image messages and posts, as well as information relating to you, such as authorship details or time of creation); usage data (e.g., page views and time spent on the site, click paths, usage intensity and frequency, device types and operating systems used, interactions with content and functions). Metadata, communication data, and procedural data (e.g., IP addresses, timestamps, identification numbers, persons involved).
- **Affected persons:** Communication partner.
- **Purposes of processing:** Communication; organizational and administrative procedures; feedback (e.g., collecting feedback via online form). Provision of our online services and user-friendliness.
- **Storage and deletion:** Deletion according to the information in the section "General information on data storage and deletion".
- **Legal basis:** Legitimate interests (Art. 6 para. 1 sentence 1 lit. f) GDPR). Contract performance and pre-contractual inquiries (Art. 6 para. 1 sentence 1 lit. b) GDPR).

Further information on processing procedures, methods and services:

- **Contact form:** When you contact us via our contact form, email, or other communication channels, we process the personal data you provide to answer and handle your request. This typically includes information such as your name, contact details, and any other information you provide that is necessary for proper processing. We use this data exclusively for the stated purpose of contacting you and communicating with you.
- **Legal basis:** Contractual performance and pre-contractual inquiries (Art. 6 para. 1 sentence 1 lit. b) GDPR), Legitimate interests (Art. 6 para. 1 sentence 1 lit. f) GDPR).