

Privacy Policy for GEPARD Websites

Privacy Policy statement for using our websites and web services.

Issue 2.2, 2021-04-08 - [Changelog](#)

Your privacy is important to us

Therefore, we have implemented a user-friendly, binding Privacy Policy to protect and handle your personal data. This policy is fully compliant to the EU General Data Protection Regulation (GDPR) applicable as of May 25th, 2018 in all member states.

This document describes which personal data we obtain, how we use and process them, and it informs you about your rights regarding your personal data.

GEPARD may change this policy from time to time by updating this page. If changed in a material way, a notice will be posted along with the updated document.

Collection and Use of Personal Information

Data collection is different for

- **anonymous users** who simply browse this website, and
- **registered users** who get access to restricted business and product information

We keep data collection at the necessary minimum. Your data will only be used in order to provide you with a user-friendly, technically functioning and secure web service and to execute your explicit requests.

If you should be asked for any information by e-mail or on our websites that you deem inappropriate or not necessary, this may result from a third part attack. Please do not provide sensible data if you are in doubt about the legitimacy or necessity of collecting these data, and inform us as soon as possible.

Data from anonymous users

What we collect

If you use this website anonymously (i.e. without logging in), we may collect for technical reasons the general use data as all other websites do. The following data set is collected by the underlying standard web server and web content management software:

- Identification information about the computer and browser you use for accessing the web content:
 - IP address (which may refer to your Internet service provider)

- Browser type and details
- Operating system type
- Language

- We may also collect information regarding your activities on our website, like
 - Referring and exit pages and
 - Time-stamped click-stream data

This list of data items may expand if the underlying standard web server and web content management applications require other or additional data for their proper technical functioning.

What we do NOT collect

With exception of the above listed data, GEPARD does not collect any further personal information from anonymous users. We will not record any of your Internet activity outside our web content with possible exception of referring and exit pages.

How we use these data

These data will only be used for technical purposes and for improving the content, use, and security of the web site but NOT for advertisement, user profiling or other commercial use.

Obtaining this basic computer and browser information is standard for any website you visit and allows to handle peculiarities and issues of your browser version, care for basic security measures, and to create general - NOT personalized - access statistics, e.g. site access by time or country.

These collected basic data are also necessary to protect you and our websites from hacker attacks, and to detect, prohibit, and analyse such attacks.

How long will these data be stored ?

Data from anonymous users will usually be deleted latest after 3 months. Longer storage may be necessary in case we have identified an attack and need these access data for investigation, proof, or during a related litigation, and subsequent legal record retention periods.

Lawfulness of processing these data

We collect and process these access data on the basis of GDPR Art.6, i.e. on our legitimate interest

- to provide you with a user-friendly website experience,
- to secure the communication between your computer and our services,
- and to protect you, our website, and our services from cyber attacks

Data from registered users

Access to restricted business information will only be granted to registered users. It is necessary to clearly authenticate and identify users requesting access to restricted information.

In addition, we will collect and process your general web site access and use data which we also

collect for anonymous users (see [above](#) for details about these data and their use and processing).

What we collect

For setting up and operating such account, we require your

- Full name
- Company name
- e-mail address
- Telephone number
- Country
- Product Installation Site (for customers)
- Installed GEPARD products and used software versions (for customers)
- Login name

These data will be explicitly provided by you on a form when applying for a login account, along with your permissions to process these data for specific and agreed purposes.

In your own discretion, you may pass additional information to us in web forms for performing specific services, like information related to a support case.

What we do NOT collect

GEPARD will not ask you for any personal or business information that is not necessary for handling your authentication and your requests.

We also do not store clear text passwords. Any password you set will be transmitted through a secured channel and only stored as irreversible hash string. Nevertheless, you should use a different and secure password for every web service.

How we use these data

All collected information will only be used to authenticate your login and to give you access to all information available under your account, and in support to carrying out the specific actions you requested.

From time to time we may use your personal information to send notices concerning your account and about changes to the information you access through your account, e.g. availability of downloads, changes of legal documents.

Supplementary information provided in request forms (e.g. support requests) will only be used for processing your request.

How long will these data be stored ?

Login accounts are linked to an existing business relation with your organization. Therefore, all related personal data must be stored for the lifetime of existing contracts and in accordance to legal and fiscal obligations, which is usually 8 to 10 years after the end of related contracts for customers and 8 years for other business partners.

Lawfulness of processing these data

We collect and process personal data of registered users on the basis of

- your explicit, written authorization to process your personal data, e.g. in (but not limited to) your account application request or support requests
- your web site use data (like for anonymous users) will be collected and processed based on GDPR Art.6, i.e. on our legitimate interests
 - to provide you with a user-friendly website experience,
 - to secure the communication between your computer and our services,
 - and to protect you, our website, and our services from cyber attacks

Contributions of registered users



We may offer you to edit, improve, and contribute articles to the technical documentation of a Product or a knowledge base. The purpose of this service is to share and build knowledge about the Product and about the field of work and expertise with other users of the Product.

If you should decide to contribute such information, you agree that this information will be visible to all other registered users of this Product. You grant the irrevocable and royalty-free right to use your information for training purposes and for their application of the Product, and for further development of the Product without fee. The pages you edit may include your user id and the date of your edit. We will also keep a history of all edits and changes.

Cookies

GEPARD's websites, online services, interactive applications, e-mail messages, and advertisements may use “cookies” and other technologies such as pixel tags and web beacons. These technologies are essential for some server applications to work, like e.g. but not restricted to a Wiki and a Cloud application.

A cookie is a small piece of data that a website asks your browser to store on your computer or mobile device. The cookie allows the website to “remember” your actions or preferences during your session or for your next visit of the website.

We respect your privacy, and only use cookies for the technical functioning and security of this website, in accordance with  [EU legislation on cookies](#) and the  [EU Opinion on Cookie Consent Exemption](#). We do NOT use them for any sort of user analysis or advertisement.

Most web browsers automatically accept cookies, but you can usually modify your browser setting to decline cookies if you prefer, or delete them whenever you like. This may prevent you from taking full advantage of the website.

Registered users must have cookies enabled in order to log-in.

Wiki Cookies

The underlying Wiki software uses the following 4 cookies:

Cookie: DokuWiki

The standard PHP session identifier. Used to hold temporary data and to avoid  CSRF attacks.

Importance: necessary; typical content: random ID

Expires: at the end of the browser session

Cookie: DOKU_PREFS

Used for remembering helpful user preferences, like the size of the editor textarea.

Importance: functional; typical content: name/value pairs in plain text

Expires: at the end of a browser session

Cookie: DW<md5-hash>

Used for authentication after login. This holds the necessary data to (re)login a previously authenticated user.

Importance: necessary for anyone who needs to log in

Typical content: encrypted username and password

Expires: at the end of a browser session

Cookie: cookielaw

Sets a flag if user has acknowledged storing of cookies.

Importance: minor; typical content: “1” if cookies have been acknowledged

Expires: never

Cloud Cookies

Nextcloud only stores cookies needed for Nextcloud to work properly. All cookies come from your Nextcloud server directly, no 3rd-party cookies will be sent to your system. Regarding GDPR, only data which contain personal data are relevant.

Cookie	Data Stored	Expires
Session cookie	session ID secret token (used to decrypt the session on the server)	24 minutes
Same-site cookies	no user-related data are stored, all same-site cookies are the same for all users on all Nextcloud instances	Never
Remember-me cookie	user id original session id remember token	15 days (can be configured)

The same-site cookies are used to determine how a request reaches the Nextcloud server. We use them to prevent CSRF attacks. No identifiable information is stored in those. The rest of the cookies are strictly used to identify the user to the system.

Protecting your personal information

We provide all reasonable administrative, technical, and physical security controls to protect your personal information, because we understand that the security of your personal information is very important.

All sensitive data and user logins are hosted on a secure HTTPS server using Secure Socket Layer (SSL) and an internationally acknowledged SSL certificate. This technology protects the confidentiality of your personal information and data while they are transmitted over the Internet. However, despite all efforts, no security controls worldwide can be guaranteed to be a 100% effective, and therefore, GEPARD cannot fully warrant the security or integrity of data stored on a web server or transmitted through the internet.

All services and features offered on GEPARD websites are hosted on virtual machines managed by an Internet Service Provider (ISP). GEPARD has sole root access to these servers but no control where these servers are located and where they are backup-ed to. We trust our ISP to have installed proper measures against unauthorized access, disclosure, alteration, and destruction.

Disclosure to Third Parties

GEPARD does not disclose your personal data to Third Parties unless

- you explicitly entitle us to do so (no hidden defaults for such entitlement)
- you put information into an area shared with other users
- it is necessary by law, legal process, litigation, and/or requests from public and governmental authorities within or outside your country of residence
- for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate
- if necessary to enforce our terms and conditions or protect our operations or users.

In the event of a merger or sale we may transfer any and all data and systems to the relevant third party. In case of a reorganization of the company all data, contracts, rights and duties may be passed to the legal successor. Registered users will be notified in such case.

Links to other websites

Our websites may contain links to other websites of interest. If you follow these links you leave our site and acknowledge that we do not have any control over these other websites. We shall not be responsible for the protection and privacy of any information you provide whilst visiting such sites, and such sites are not governed by this privacy statement. You should exercise caution and look at the privacy statement applicable to the website in question.

We do our best to carefully select and decide on external links at the time of editing a web page. But as contents of other websites continuously change, and referred websites may be

discontinued, reassigned, or redirected to other organizations and sites, we cannot and shall not be responsible for using external links on our web site and for the content of these Third Party sites.

User Rights - Controlling your personal information

According to applicable law you have the right to

- check if and which personal data we store about you,
- request a copy of such data,
- request the rectification, completion, or erasure of your personal data which are wrong or have not been processed lawfully,
- request us to restrict the processing of your personal data,
- object the processing of your personal data,
- withdraw a previous agreement to process your personal data (which does not affect the lawfulness of the data processing until the time of withdrawal)
- request data portability to transfer your personal data
- request the identity of third parties to which your personal data are being transmitted
- lodge a complaint with the Austrian Data Protection Agency

These rights may be subject to certain limitations and requirements according to applicable law, e.g. if these data are necessary

- for compliance with our legal and fiscal obligations
- for fulfilling existing contracts with your organization
- for the establishment, exercise or defence of legal claims
- for exercising our right of freedom of expression and information

Form of requests

All such requests shall be submitted in writing to the address [below](#).

If you are an anonymous surfer on our websites, the data collected about you are only linked to your IP address and not to any natural person or organization. Therefore, your request can only be processed if you provide

- the IP address which your request is based on
- the statement and proof that you were the sole owner of this IP address during the requested time period
- if the owner of the IP address is not a natural person, the request will only be accepted from an authorized representative of this organization
- your full contact credentials including full name, postal address, e-mail address, and telephone number in order to verify the legitimacy and authenticity of the request

If you are a registered user, customer, supplier or other business partner, your request must include all credentials necessary for your unambiguous identification including

- your full contact credentials including full name, postal address, e-mail address, and

telephone number in order to verify the legitimacy and authenticity of the request

- requests on behalf of an organization or concerning data related to an organization will only be accepted from an authorized representative of this organization

Processing of your requests

Before releasing any of your data or applying any changes to your data and related processes, we will contact you to verify the legitimacy of the request, in order to protect you and us from unauthorized third party interference.

We will inform you on completion of your request.

Legitimate requests will usually be processed within a month.

Excessive and/or complex requests may take longer but will be completed within 3 months. We will inform you on such delay.

Processing of legitimate and reasonable requests is free of charge. But for requested additional data copies, frequent and/or excessive requests, a reasonable fee based on administrative costs will be charged.

Any request regarding personal data will trigger a separate data processing action and produce a separate set of personal information related to this request, which will be stored for a legal record retention period of (currently) 8 years.

Request from a customer may be stored up to 10 years.

Contact

The responsibility for the collection, use, and processing of your personal data on GEPARD websites and web services resides in

GEPARD, J. Scheiber KG
Florian-Berndl-Gasse 52
1220 Vienna, Austria
Europe



+43 1 513 08 100



+43 1 513 08 700



privacy@gepard.at



[Impressum](#)