

Privacy Statement – Keronic

Keronic B.V. and Keronic Software B.V. (hereinafter: “Keronic”, “we”, “us”, or “our”), located at Utopialaan 40, 5232 CE 's-Hertogenbosch, The Netherlands, are responsible for the processing of personal data as described in this Privacy Statement.

This Privacy Statement applies to individuals located in the European Economic Area (EEA) and the United Kingdom (UK). Keronic recognized the importance of information security and the protection of privacy. This privacy statement is based on the principles of the GRDP, ISO27001 and are embedded in Keronic’s Information Security Management System (ISMS), according to the following principles:

- There are processes in place according to ISO27001 and our ISMS to secure these statements (for example retention periods).
- The organization adheres to the principles of privacy by design and privacy by default;
- A risk assessment demonstrates how data is used within the organization's processes;
- Measures have been implemented to ensure adequate protection of data at rest and data in transit;
- Processes have been adapted to ensure that data is not retained for longer than necessary to provide the services;
- For verification purposes, the implemented measures and controls are documented in a Compliance Statement, which is available upon request.

Contact details

- Website: <https://www.keronic.com>
- Phone: +31 73 833 01 01
- Email: info@keronic.com
- Data Protection Officer: Keronic’ Security Officer
- Email: security@keronic.com

1. Personal data we process

We process personal data when you:

- Use our services;
- Contact us;
- Engage with us in a business context.

This may include:

- First and last name
- Business email address
- Telephone number
- Company name and job title
- Any information you provide in correspondence

2. Purpose and legal basis for processing

We process personal data for the following purposes and legal grounds:

a. To provide our software development services and products

Legal basis: performance of a contract

b. To communicate with clients, prospects, and partners

Legal basis: legitimate interest

c. To manage customer relationships via CRM systems

Legal basis: legitimate interest

d. To comply with legal obligations

Legal basis: legal obligation

e. Recruitment and hiring processes

Legal basis: legitimate interest and/or consent

3. Use of CRM and service providers

We use third-party service providers, including CRM systems and IT hosting providers, to support our business operations. These providers may process personal data on our behalf as data processors. We ensure that:

- Appropriate data processing agreements are in place.
- Data is processed securely and confidentially.

4. International data transfers

Where personal data is transferred outside the EEA or the UK, we ensure appropriate safeguards are in place, such as:

- Standard Contractual Clauses (SCCs) approved by the European Commission.
- UK International Data Transfer Agreement (IDTA), where applicable.

5. Retention periods

We retain personal data only for as long as necessary for the purposes described above:

- Customer contact and business data: information acquired through contact forms will be automatically deleted up to 12 months after last contact.
- Recruitment data: up to 4 weeks after completion of the process, unless consent is given for longer retention and when the recruitment process leads to an employment relationship. Where consent for longer retention has been provided, recruitment data will be retained for a maximum of 1 year.
- Contract-related data: retained in accordance with legal obligations.

6. Cookies

We use functional and limited analytical cookies to ensure the proper functioning of our website and to improve user experience. You can manage or disable cookies via your browser settings.

7. Your rights

Under the GDPR and UK GDPR, you have the right to:

- Access your personal data.
- Rectify inaccurate data.
- Request deletion of your data.
- Restrict processing.
- Object to processing.
- Request data portability.
- Withdraw consent (where applicable).

Requests can be sent to: security@keronic.com
We will respond within one month.

8. Complaints

- If you are located in the Netherlands, you may file a complaint with the Dutch Data Protection Authority:
<https://autoriteitpersoonsgegevens.nl>
- If you are located in the United Kingdom, you may contact the UK Information Commissioner's Office (ICO):
<https://ico.org.uk>
- If you are located in Germany, you may contact the German Federal Commissioner for Data Protection and Freedom of Information (BfDI)
<https://www.bfdi.bund.de>

9. Security

We take appropriate technical and organizational measures to protect personal data against:

- Loss.
- Misuse.
- Unauthorised acces.
- Disclosure or alteration.

10. Children

Our services are not intended for individuals under the age of 16. We do not knowingly collect personal data from children without parental consent.

11. Changes

We may update this Privacy Statement from time to time. The latest version will always be published on our website.

12. Responsible disclosure

The security of our systems is our top priority. We kindly ask you to report any weaknesses so we can improve our systems. Please do the following:

- Email your findings to security@keronic.com. Encrypt your e-mail.
- Do not exploit the vulnerability or issue you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or by deleting or modifying other people's data;
- Do not disclose the issue to others until it has been resolved;
- Do not carry out attacks against physical security, use social engineering, distributed denial-of-service attacks, spam, or third-party applications; and
- Provide sufficient information for us to reproduce the issue so that we can resolve it as quickly as possible. In most cases, the IP address or URL of the affected system and a description of the vulnerability will be sufficient, but more detailed information may be required for complex vulnerabilities.

What we promise:

- We will respond to your report within one business week with our assessment of the report and an expected date for a resolution;
- If you have followed the instructions above, we will not take legal action against you in relation to the report;
- We will treat your report as strictly confidential and will not share your personal information with third parties without your consent;
- We will keep you informed of our progress in resolving the issue;
- In any public information about the reported issue, we will credit you as the discoverer of the issue (unless you prefer otherwise); and
- As a token of our appreciation for your help, we offer a reward for every report of a security issue that we were previously unaware of. The amount of the reward is determined based on the severity of the vulnerability and the quality of the report. As a reward we will honor you in our Hall of Fame forever.

We aim to resolve all issues as quickly as possible, and we would like to play an active role in the eventual publication about the issue once it has been resolved.