Privacy policy for the whistleblower platform

In the following statement, we would like to inform you about how we collect, process and use personal data as part of our whistleblower system when you provide us with a report via a form on our platform. Our whistleblowing system has been implemented to ensure that all reports received are investigated and processed in a transparent and fair manner. Please take a moment to read this Privacy Notice carefully before submitting a report.

1 Identity and contact details of the controller and its representative

The controller responsible for data processing is

apt Holding GmbH
Rheinpromenade 11
40789 Monheim am Rhein
Monheim am Rhein, Germany
Phone: +49 2173 / 297 02 10

If you have any questions, you can reach us at info.holding@apt-alu-products.com

2. contact details of the data protection officer

Our data protection officer can be contacted at datenschutz@apt-alu-products.com

3 Purposes and legal bases of the processing of personal data

- Operation of the reporting office and management of the procedure

The processing of personal data in the context of the whistleblower system serves to ensure the operation of the reporting channel, to manage the procedure for investigating and assessing reports and to take appropriate follow-up measures based on the results of the investigation. The legitimate interest lies in particular in clarifying and sanctioning misconduct that has been committed.

Violations that are reported as misconduct via an internal procedure can be:

1. conduct that constitutes a criminal offense against the interests of the company (in particular fraud and misconduct in relation to accounting and internal accounting controls, auditing offenses, corruption, banking and financial crime, prohibited insider trading),

2. conduct that violates human rights (e.g. exploitation of favorable production conditions abroad by accepting child labor), environmental protection concerns or regulations under the General Equal Treatment Act,

3. conduct that violates the company's internal ethical rules.

- Consent of the whistleblower

In some cases, it may be necessary to disclose information about your identity or other circumstances that allow conclusions to be drawn about your identity. This is only permitted if the disclosure is necessary for follow-up measures, such as investigations or legal action, and the disclosing person has previously expressly consented to this disclosure in text form. Consent would be obtained separately for each individual disclosure of personal data.

- Data processing for the purposes of the employment relationship

If you yourself have been registered by a third party, the processing of your personal data also serves to decide on the establishment, implementation and termination of an employment relationship and the exercise or fulfillment of rights and obligations arising from legal norms. The relevant legal basis for this arises from the execution of the employment relationship and from the processing necessary for the detection of criminal offenses, provided that there are documented, justified grounds for suspicion and the data subject's legitimate interest in the exclusion of processing does not prevail.

- Disclosure to the competent authorities

The disclosure of information about the identity of both the reporting person and the persons who are the subject of a report, as well as other persons named in the report, serves to enable an efficient investigation and processing of the information and to initiate the necessary legal or internal action.

4 Categories of personal data

The whistleblower system is used on a voluntary basis. We collect the following personal data and information when you submit a report:

- Information for personal identification of the whistleblower, such as first and last name, gender, address, telephone number and e-mail address;
  Employee status of apt Holding GmbH and its affiliated companies;
- Information on affected persons, i.e. natural persons who are designated in a report as a person who committed the violation or with whom the designated person is associated. Such information includes first and last name, gender, address, telephone number and e-mail address or other information that enables identification;
- Information about violations that may allow conclusions to be drawn about a natural person.

5. recipients or categories of recipients of the personal data

Access to the data is restricted to a very narrow circle of expressly authorized employees of apt Holding GmbH and its affiliated companies as well as the employees of the provider of the whistleblowing system. In certain cases, it may be necessary to pass on data to external bodies, such as law enforcement authorities.

Our whistleblowing platform is made available on an external reporting channel "EQS Integrity Line" of the EQS Group AG whistleblowing system. The anonymity of your reports is guaranteed throughout by technical and organizational measures. Reports are end-to-end encrypted, hosted on ISO 27001 certified German servers. You can find EQS's general privacy policy here: https://www.eqs.com/de/ueber-eqs/datenschutz/.

The EQS Integrity Line privacy policy can be found here:

https://eqs-ethics-line.com/index.php?action=showFooterLink&id=10

Depending on the nature of the case and the legal requirements, information about the identity of the whistleblower, the persons who are the subject of a report and other persons named in the report or other circumstances that allow conclusions to be drawn about their identity may have to be passed on to certain recipients. These may include law enforcement authorities, administrative authorities, courts or certain supervisory authorities.

6. transfer of personal data to third countries or international organizations

Data processing will primarily take place in the EU. A transfer to third countries will only take place on the basis of suitable or appropriate data protection guarantees for the protection of data subjects, e.g. by concluding the so-called EU standard contractual clauses (SCCs) and, if necessary, additional technical and organizational measures.

7. storage periods for personal data

Personal data will be stored until the final assessment of the notice and then for a further two years. At the end of this period, this data will be deleted in accordance with legal requirements. If a reported violation proves to be unfounded, the data collected will be deleted immediately.

In addition, personal data may have to be retained in accordance with criminal law for the period during which claims can be asserted against the person accused of misconduct (statutory limitation period of three or up to thirty years). Other mandatory statutory retention periods (e.g. under tax, commercial or duty law) may also oblige us to store your data for a longer period.

8. the existence of the right of access, rectification, erasure, restriction of processing, objection and data portability

Under European data protection law, you and the persons named in the notice have the right of access, rectification, erasure, restriction of processing and, in certain cases, the right to data portability.

Please note that, depending on the content of your notification, certain rights may be restricted under the GDPR. Art. 23 GDPR allows Member States to take legal measures to restrict certain rights and obligations if this is necessary and proportionate, for example to safeguard national security, defense, public security interests, the prevention, investigation, detection and prosecution of criminal offenses or breaches of professional ethics, the protection of important objectives of general public interest, the protection of the independence of the judiciary and judicial proceedings, the protection of data subjects or the rights and freedoms of others.

If you have any questions or concerns about your rights as a data subject, we recommend that you contact our data protection officer at datenschutz@apt-alu-products.com.

9. the right to withdraw consent to the disclosure of personal data at any time

If you have consented to the disclosure of information about your identity or other circumstances that allow conclusions to be drawn about it, you can revoke this consent.

10. the right to lodge a complaint with a supervisory authority

If you are of the opinion that the handling of your personal data violates data protection regulations, you can lodge a complaint with the competent data protection authority at any time. This could be the authority responsible for your usual place of residence, your place of work or the place of the suspected infringement. Please note that this right is independent of any other available administrative or judicial remedy.

11. security of your personal data

We take all reasonable necessary technical and organizational measures to ensure the security of your personal data and to protect it from unauthorized access and misuse.