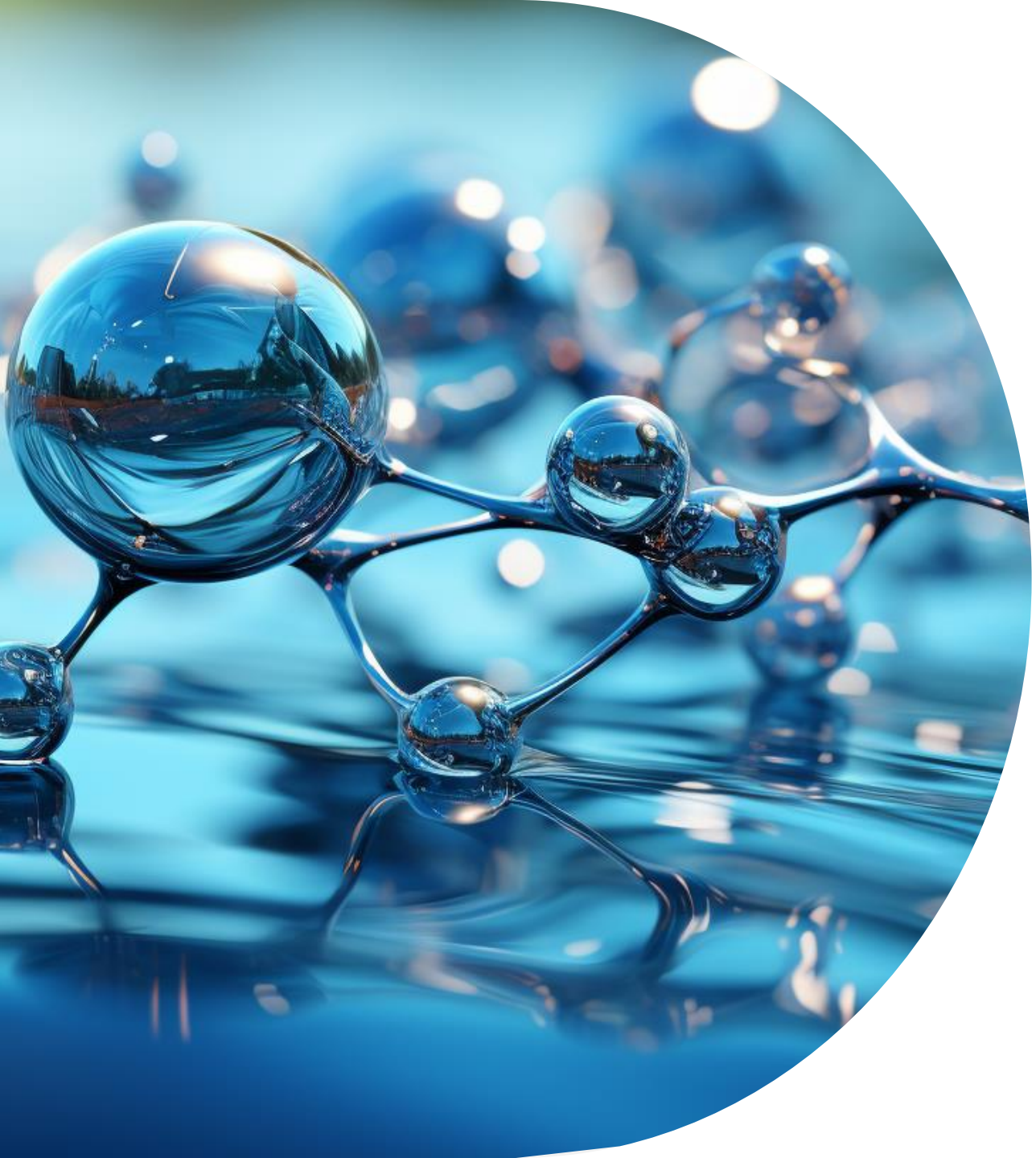


Sep. 2023

H2APEX Group SCA

CODE OF CONDUCT

Data Privacy & Information Security

DATA PRIVACY & INFORMATION SECURITY

We recognize the ongoing digitalization as a valuable opportunity for our company and the goals we are pursuing. Therefore, it is important to protect the information we process.

We are dedicated to preserving the confidentiality, integrity, and accessibility of business information by implementing suitable technical and organizational security measures. It falls upon our employees to uphold this commitment, ensuring adherence to all guidelines and regulations that bolster information security.

We adhere strictly to relevant national data protection laws aimed at safeguarding individuals' privacy. Thus, personal data is utilized by us solely when justified, and only maintained while the justification persists. Such justification may particularly arise if the individual has provided documented consent, if legal obligations necessitate its use, or if there is a legitimate interest in its application. In cases of legitimate interest, we also conduct a thorough, documented assessment to balance interests.

This document serves as a crucial guide to effectively safeguarding information and data. In case of any uncertainties or questions, reach out to the Compliance department.

H2APEX

PRINCIPLES OF DATA PROTECTION

What is personal data?

Personal data according to the GDPR (General Data Protection Regulation) is information that can be used to directly or indirectly identify a person. This encompasses various identifiers such as names, ID numbers, location data, and online identifiers, along with characteristics pertinent to an individual's physical, physiological, genetic, mental, economic, cultural, or social identity.

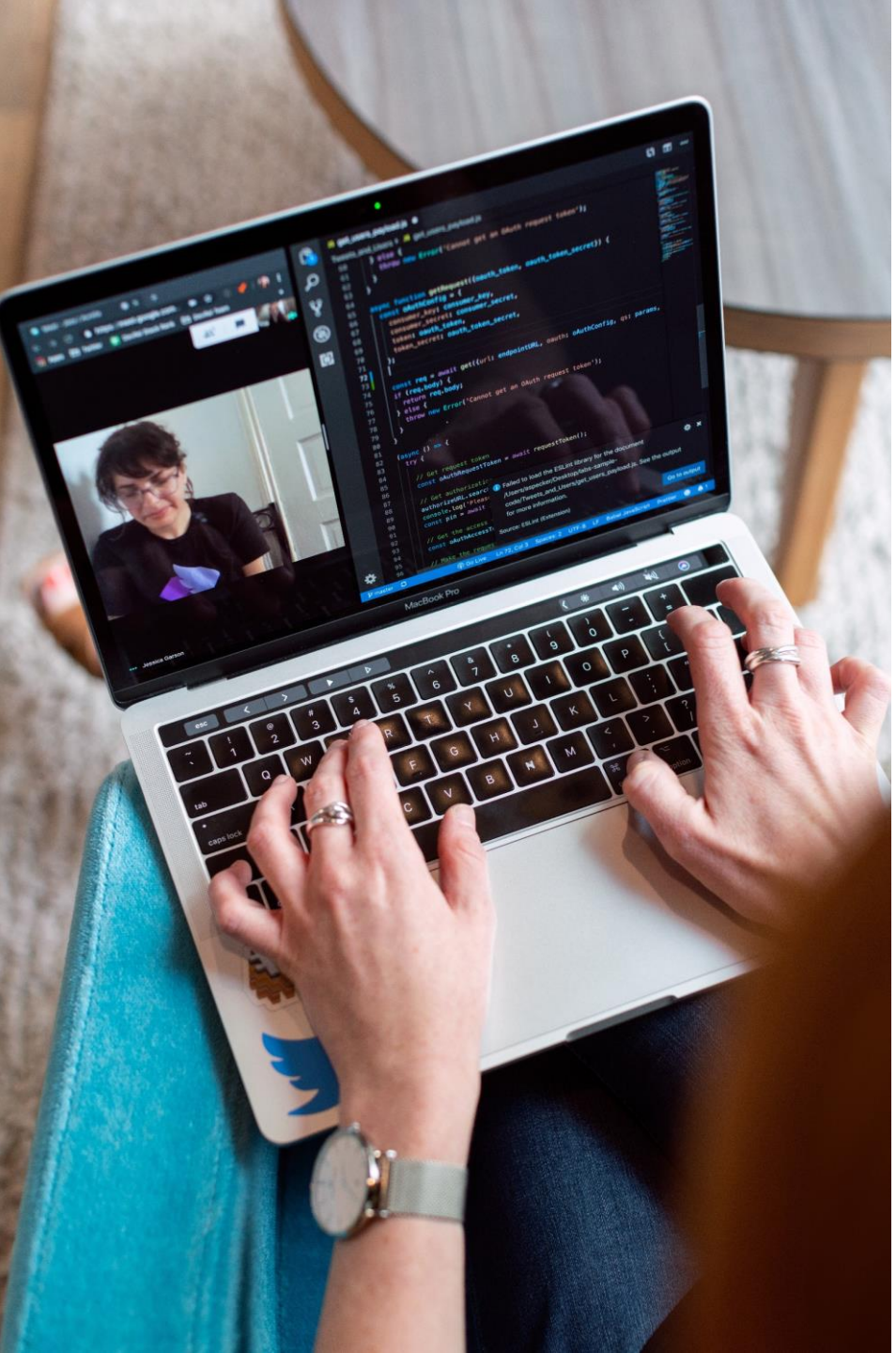
Put simply, any information that can unveil the identity of an individual qualifies as personal data.

Special categories of personal data

The GDPR distinguishes "special categories of personal data," often termed "sensitive data," due to their intrinsic sensitivity, necessitating heightened protection measures. These categories bear an elevated risk of infringing upon individuals' fundamental rights and freedoms if mishandled.

Sensitive data encapsulates details concerning racial or ethnic origin, political affiliations, religious or philosophical beliefs, trade union memberships, as well as genetic and biometric data utilized for unique identification, health-related information, and data characterizing a person's sexual life or orientation.

Processing of these special categories of data is generally prohibited unless one of the exceptions listed in the GDPR applies, e.g., if the data subject has given explicit consent or if it is necessary for specific legal or medical reasons. It is important to take special care when handling and processing this data.



PRINCIPLES FOR PROCESSING PERSONAL DATA

When processing personal data, we always adhere to the following principles:

- Personal data must be processed lawfully and in good faith, ensuring transparency for the data subjects, making it clear how their data is being used.
- Data should be collected for well-defined, explicit and lawful purposes and must not be further processed in ways incompatible with those purposes.
- Only data that is essential for the intended purpose should be collected and processed.
- Data must be accurate and, if necessary, kept up to date. Immediate steps should be taken to amend or erase inaccurate or incomplete data.
- Personal data should be stored in a way that allows the identification of data subjects only as long as necessary for the intended processing purposes.
- Appropriate technical and organizational measures should be implemented to safeguard personal data, protecting against unauthorized access, illicit usage, and accidental loss or destruction.
- The data controller must be able to demonstrate compliance with these principles.

PRINCIPLES OF DATA PROTECTION

Processors, service providers and data transfer

We are particularly careful when selecting service providers and suppliers who have access to personal data. If they process data on behalf of H2APEX, we ensure that the so-called processor has taken appropriate measures to ensure that all processing is carried out in compliance with the requirements of the GDPR and with regard to the protection of the rights of data subjects. This means that when selecting our service providers, in addition to data processing expertise, we also take into account the technical and organizational measures (TOMs for short; by this we mean all measures, whether physical or digital, that help to protect information and data)* implemented by the processor.

The transfer of personal data to third parties is only permitted with legal permission or with the consent of the data subject. For data recipients outside the EU or the European Economic Area (EEA), we implement special measures to protect data subjects. We refrain from transferring data to countries without adequate data protection or comparable guarantees.

Data protection incidents

If the protection of personal data is breached, for example due to IT problems or the loss of unencrypted data media, we inform the responsible data protection authority within 72 hours. In certain cases, the data subjects are also notified of the incident.

Data subject rights

Data subjects have several rights regarding the processing of their personal data. These rights include transparency and information access, the right to correct inaccuracies in their data, and the ability to revoke or limit the consent given for data processing. We are committed to facilitating the exercise of these rights by data subjects. Upon justified request, we will promptly stop processing and storing the individual's personal data, ensuring that their rights are fully respected and upheld.

*** Upon request, we provide our business partners with an overview of our technical and organizational measures.**

RESPONSIBILITY MEANS ACTION

If potential violations of this Code of Conduct, laws or internal policies are noticed, we ask that they be reported to the manager, executive management or the compliance department. If it is uncomfortable to address these issues directly, it is possible to submit the tip anonymously via the whistleblower system.

Every report from a whistleblower will be handled with utmost confidentiality and in strict compliance with all applicable legal provisions. Whistleblowers will not face any adverse consequences or reprisals as a result of their disclosure.

compliance@apex-energy.de

www.apex-group.de/compliance