DATA SECURITY

Data security is one of the two funding priorities of the Prototype Fund.

Data security tools help protecting sensitive data from l**oss, unauthorised access or manipulation**. The aim is therefore to prevent security-relevant failures, interruptions or data leaks due to software errors as well as to ward off attackers who exploit vulnerabilities, e.g. through malware.

Data security projects include, for example, the implementation of encryption protocols and tools for software testing or for checking data integrity.

A particularly important objective of data security is **data protection, i.e. the protection of personal data such as e-mail addresses, social security numbers or location data**. Data protection is anchored in the right to informational self-determination, according to which every person is entitled to determine the disclosure and use of their own data. Possible negative consequences of disclosing personal data range from its sale for advertising purposes to identity theft and political persecution. **Protecting non-personal data can also be in the public interest**. This is particularly the case if the operation of critical infrastructures depends on them, the failure of which could lead to supply bottlenecks or even endanger public safety.

Data security is implemented effectively and efficiently from the very beginning of the development process. The Prototype Fund therefore promotes software development according to the principle of security by design and privacy by design. Secure data processing is built into the design of new software components right at the start. Data security can be achieved particularly well with open source software because it is **developed transparently and collaboratively and can be reviewed by third parties at any time**.

PROTOTYPE FUND