CLAIMS

1. A method of controlling access to data stored in a data repository, the method comprising:

negotiating by a set of artificial intelligence agents to generate a set of smart contract terms, wherein the set of artificial intelligence agents includes an artificial intelligence agent representing an entity having the data repository;

performing a compliance check on the smart contract terms against a data regulation;

if the compliance check is successful, deploying a smart contract comprising the set of smart contract terms; and

controlling access to the data stored in the data repository using the smart contract, wherein the artificial intelligence agent grants a user access to the data stored in the data repository based on the smart contract.

2. The method according to claim 1, wherein controlling access to the data stored in the data repository using the smart contract comprises the artificial intelligence agent of the set of artificial intelligence agents monitoring user actions on performed on the data stored in the data repository and if a user action violates a term of the set of smart contract terms, denying access by the user to the data stored in the data repository.

3. The method according to claim 1, wherein controlling access to the data stored in the data repository using the smart contract comprises the artificial intelligence agent of the set of artificial intelligence agents performing a transformation on the data stored in the data repository and providing transformed data to a user.

4. The method according to claim 3, wherein the transformation is defined by a term of the set of smart contract terms.

5. The method according to any preceding claim, wherein the negotiating by the set of artificial intelligence agents to generate a set of smart contract terms is based on data sensitivity, data usage purposes and data access permissions.

6. The method according to any preceding claim, wherein controlling access to the data stored in the data repository using the smart contract comprises detecting a data privacy violation and triggering a data privacy protection mechanism in response to detecting the data privacy violation.

7. The method according to any preceding claim, wherein controlling access to the data stored in the data repository using the smart contract comprises detecting bias in data accessed from the data repository and initiating a bias mitigation process in response to detecting bias in data accessed from the data repository.

8. The method according to any preceding claim, wherein controlling access to the data stored in the data repository using the smart contract comprises detecting malicious elements in data accessed from the data repository and initiating a malicious data cleansing process in response to detecting malicious elements in data accessed from the data repository.

9. The method according to any preceding claim, wherein deploying the smart contract comprises storing the smart contract on a distributed ledger.

10. The method according to any preceding claim, further comprising detecting a change in the data regulation and adapting the set of smart contract terms in response to detecting the change in the data regulation.

11. The method according to any preceding claim, further comprising updating an audit log indicating data accessed in the data repository.

12. A computer readable medium storing processor executable instructions which when executed on a processor cause the processor to carry out a method according to any one of claims 1 to 11.

13. A computer system for controlling access to data stored in a data repository, the computer system configured to implement a plurality of artificial intelligence agents which implement a method according to any one of claims 1 to 11.

14. The computer system according to claim 13, further comprising a compliance system configured to monitor compliance of the artificial intelligence agents with a data regulation.