THE INVENTION CLAIMED IS:

1. A computer-implemented method, comprising:

receiving, by a consent database, a first data request for user data associated with a user from a requester system, the user data stored in a user data database separate from the consent database;

communicating, by the consent database, a consent request to the requester system for display to the user on a user device associated with the user;

receiving, by the consent database, a consent response from the requester system based on input from the user device, the consent response indicating consent from the user to share the user data requested in the first data request;

storing, by the consent database, consent data associated with the consent response for the user data requested in the first data request in an immutable ledger;

receiving, by the consent database, a consent verification request from the user data database, the consent verification request based on a second data request for the user data from the requester system to the user data database;

verifying, by the consent database, the consent verification request based on the consent data stored in the immutable ledger; and

communicating, by the consent database, a consent verification response based on verifying the consent verification request to the user data database, the consent verification response indicating consent from the user to share the user data from the user data database with the requester system.

2. The method of claim 1, further comprising:

receiving, by the consent database, from the requester system, utilization data associated with consented use of user data; and

storing, by the consent database, the utilization data associated with the user data in the immutable ledger.

3. The method of claim 2, further comprising:

receiving, by the consent database, from the user data database, distribution data associated with a data access of the user data from the requester system; and

storing, by the consent database, the distribution data associated with the user data in the immutable ledger.

4. The method of claim 3, further comprising:

comparing, by the consent database, the distribution data associated with the user data with the consent data associated with the user data;

determining, by the consent database, compliance of the distribution data to conditions of the consent data; and

storing, by the consent database, an indication of compliance of the distribution data in the immutable ledger.

5. The method of claim 2, further comprising:

comparing, by the consent database, the utilization data associated with the user data with the consent data associated with the user data;

determining, by the consent database, compliance of the utilization data to conditions of the consent data; and

storing, by the consent database, an indication of compliance of the utilization data in the immutable ledger.

6. The method of claim 5, further comprising:

receiving, by the consent database, an audit request associated with the user data from the user data database; and

communicating, by the consent database, the indication of compliance of the utilization data associated with the user data to the user data database.

7. The method of claim 1, further comprising:

receiving, by the consent database, a revocation request of a consent associated with the user data from the user device;

updating, by the consent database, the consent response based on the revocation request; and

communicating, by the consent database, the updated consent response to the user data database.

8. A system for managing consent, the system comprising at least one server computer including at least one processor, the at least one server computer programmed and/or configured to:

receive a first data request for user data associated with a user from a requester system, the user data stored in a user data database separate from a consent database;

communicate a consent request to the requester system for display to the user on a user device associated with the user;

receive a consent response from the requester system based on input from the user device, the consent response indicating consent from the user to share the user data requested in the first data request;

store consent data associated with the consent response for the user data requested in the first data request in an immutable ledger;

receive a consent verification request from the user data database, the consent verification request based on a second data request for the user data from the requester system to the user data database;

verify the consent verification request based on the consent data stored in the immutable ledger; and

communicate a consent verification response based on verifying the consent verification request to the user data database, the consent verification response indicating consent from the user to share the user data from the user data database with the requester system.

9. The system of claim 8, wherein the at least one server computer is programmed and/or configured to:

receive, from the requester system, utilization data associated with consented use of user data; and

store the utilization data associated with the user data in the immutable ledger.

10. The system of claim 9, wherein the at least one server computer is programmed and/or configured to:

receive, from the user data database, distribution data associated with a data access of the user data from the requester system; and

store the distribution data associated with the user data in the immutable ledger.

11. The system of claim 10, wherein the at least one server computer is programmed and/or configured to:

compare the distribution data associated with the user data with the consent data associated with the user data;

determine compliance of the distribution data to conditions of the consent data; and

store an indication of compliance of the distribution data in the immutable ledger.

12. The system of claim 9, wherein the at least one server computer is programmed and/or configured to:

compare the utilization data associated with the user data with the consent data associated with the user data;

determine compliance of the utilization data to conditions of the consent data; and

store an indication of compliance of the utilization data in the immutable ledger.

13. The system of claim 12, wherein the at least one server computer is programmed and/or configured to:

receive an audit request associated with the user data from the user data database; and

communicate the indication of compliance of the utilization data associated with the user data to the user data database.

14. The system of claim 8, wherein the at least one server computer is programmed and/or configured to:

receive a revocation request of a consent associated with the user data from the user device;

update the consent response based on the revocation request; and

communicate the updated consent response to the user data database.

15. A computer program product comprising at least one non-transitory computer-readable medium including one or more program instructions that, when executed by at least one processor, cause the at least one processor to:

receive a first data request for user data associated with a user from a requester system, the user data stored in a user data database separate from a consent database;

communicate a consent request to the requester system for display to the user on a user device associated with the user;

receive a consent response from the requester system based on input from the user device, the consent response indicating consent from the user to share the user data requested in the first data request;

store consent data associated with the consent response for the user data requested in the first data request in an immutable ledger;

receive a consent verification request from the user data database, the consent verification request based on a second data request for the user data from the requester system to the user data database;

verify the consent verification request based on the consent data stored in the immutable ledger; and

communicate a consent verification response based on verifying the consent verification request to the user data database, the consent verification response indicating consent from the user to share the user data from the user data database with the requester system.

16. The computer program product of claim 15, wherein the one or more program instructions further cause the at least one processor to:

receive, from the requester system, utilization data associated with consented use of user data; and

store the utilization data associated with the user data in the immutable ledger.

17. The computer program product of claim 16, wherein the one or more program instructions further cause the at least one processor to:

receive, from the user data database, distribution data associated with a data access of the user data from the requester system; and

store the distribution data associated with the user data in the immutable ledger.

18. The computer program product of claim 17, wherein the one or more program instructions further cause the at least one processor to:

compare the distribution data associated with the user data with the consent data associated with the user data;

determine compliance of the distribution data to conditions of the consent data; and

store an indication of compliance of the distribution data in the immutable ledger.

19. The computer program product of claim 16, wherein the one or more program instructions further cause the at least one processor to:

compare the utilization data associated with the user data with the consent data associated with the user data;

determine compliance of the utilization data to conditions of the consent data; and

store an indication of compliance of the utilization data in the immutable ledger.

20. The computer program product of claim 19, wherein the one or more program instructions further cause the at least one processor to:

receive an audit request associated with the user data from the user data database; and

communicate the indication of compliance of the utilization data associated with the user data to the user data database.