CLAIMS

1. A method, comprising:

receiving, at a cloud data privacy service, a request from a user device to permit a first data processor to access private data associated with the user, the request comprising:

a request for a first data access block relating to the private data; and

a data filter describing one or more access parameters relating to the first data processor and the private data;

generating the first data access block, at the cloud data privacy service, based on the private data and the data filter;

transmitting the first data access block from the cloud privacy service to the user device, wherein the user device is configured to transmit the first data access block to the first data processor;

receiving, at the cloud data privacy service, a request from the first data processor for the private data, the request comprising the first data access block; and

determining, at the cloud data privacy service, that the first data access block received from first data processor is valid, and in response granting the first data processor at least partial access to the private data.

2. The method according to the preceding claim, wherein a scope of the at least partial access to the private data granted to the first data processor is based on the first data access block.

3. The method according to any of the preceding claims, further comprising:

determining, at the cloud data privacy service, based on the first data access block received from the first data processor, that the data filter specifies user approval prior to granting the first data processor access to the private data, and in response:

transmitting from the cloud data privacy service to the user device a request for approval; and

receiving, at the cloud data privacy service from the user device, a message indicating approval.

4. The method according to the preceding claim, wherein the determining, at the cloud data privacy service, that the data filter specifies user approval further comprises:

determining, based on the first data access block received from the first data processor, an identifier for the data filter; and

retrieving from a filter repository the data filter based on the identifier.

5. The method according to the preceding claim, wherein the data filter is generated based on input from the user at the user device.

6. The method according to any of the preceding claims, wherein the determining, at the cloud data privacy service, that the first data access block received from first data processor is valid comprises:

determining that a digital signature for the first data access block is valid.

7. The method according to any of the preceding claims, wherein the user device is configured to transmit an address for the cloud privacy service to the first data processor along with the first data access block, and wherein the first data processor is configured to transmit the request for the private data to the cloud privacy service based on the address.

8. The method according to any of the preceding claims, further comprising:

providing, by the first data processor to a second data processor, access to at least a portion of the private data, comprising:

generating, at the cloud data privacy service based on the first data access block, a second data access block relating to a second data processor;

transmitting, from the cloud data privacy service to the first data processor, the second data access block, wherein the first data processor is configured to provide the second data access block to the second data processor;

receiving, at the cloud data privacy service from the second data processor, a request to access the at least the portion of the private data, the request comprising the second data access block; and

determining, at the cloud data privacy service, that the second data access block received from the second data processor is valid, and in response granting the

second data processor at least partial access to the at least the portion of the private data.

9. The method according to the preceding claim, wherein the second data access block reflects access to only a portion of the private data for the second data processor.

10. The method according to any of the preceding claims, further comprising:

storing the first data access block in a data access block registry.

11. The method according to any of the preceding claims, wherein the first data processor is granted access to the private data for a limited duration, and wherein the first data processor is configured to remove the private data after the limited duration expires.

12. The method according to any of the preceding claims, wherein the cloud privacy service operates in a public cloud environment independent from the first data processor, and wherein the private data is maintained in the public cloud environment.

13. A system, comprising:

a processor; and

a memory storing a program, which, when executed on the processor, performs an operation, the operation comprising:

receiving, at a cloud data privacy service, a request from a user device to permit a first data processor to access private data associated with the user, the request comprising:

a request for a first data access block relating to the private data; and

a data filter describing one or more access parameters relating to the first data processor and the private data;

generating the first data access block, at the cloud data privacy service, based on the private data and the data filter;

transmitting the first data access block from the cloud privacy service to the user device, wherein the user device is configured to transmit the first data access block to the first data processor;

receiving, at the cloud data privacy service, a request from the first data processor for the private data, the request comprising the first data access block; and

determining, at the cloud data privacy service, that the first data access block received from the first data processor is valid, and in response granting the first data processor at least partial access to the private data.

14. The system according to the preceding claim, wherein a scope of the at least partial access to the private data granted to the first data processor is based on the first data access block.

15. The system according to any of the two preceding claims, the operation further comprising:

determining, at the cloud data privacy service, based on the first data access block received from the first data processor, that the data filter specifies user approval prior to granting the first data processor access to the private data, and in response:

transmitting from the cloud data privacy service to the user device a request for approval; and

receiving, at the cloud data privacy service from the user device, a message indicating approval.

16. The system according to any of the preceding claims 13 to 15, the operation further comprising:

providing, by the first data processor to a second data processor, access to at least a portion of the private data, comprising:

generating, at the cloud data privacy service based on the first data access block, a second data access block relating to a second data processor;

transmitting, from the cloud data privacy service to the first data processor, the second data access block, wherein the first data processor is configured to provide the second data access block to the second data processor;

receiving, at the cloud data privacy service from the second data processor, a request to access the at least the portion of the private data, the request comprising the second data access block; and

determining, at the cloud data privacy service, that the second data access block received from second data processor is valid, and in response granting the second data processor at least partial access to the at least the portion of the private data.

17. A non-transitory computer program product, the computer program product comprising:

a computer-readable storage medium having computer-readable program code embodied therewith, the computer-readable program code executable by one or more computer processors to perform an operation, the operation comprising:

receiving, at a cloud data privacy service, a request from a user device to permit a first data processor to access private data associated with the user, the request comprising:

a request for a first data access block relating to the private data; and

a data filter describing one or more access parameters relating to the first data processor and the private data;

generating the first data access block, at the cloud data privacy service, based on the private data and the data filter;

transmitting the first data access block from the cloud privacy service to the user device, wherein the user device is configured to transmit the first data access block to the first data processor;

receiving, at the cloud data privacy service, a request from the first data processor for the private data, the request comprising the first data access block; and

determining, at the cloud data privacy service, that the first data access block received from first data processor is valid, and in response granting the first data processor at least partial access to the private data.

18. The computer program product according to the preceding claim, wherein a scope of the at least partial access to the private data granted to the first data processor is based on the first data access block.

19. The computer program product according to any of the two preceding claims, the operation further comprising:

determining, at the cloud data privacy service, based on the first data access block received from first data processor, that the data filter specifies user approval prior to granting the first data processor access to the private data, and in response:

transmitting from the cloud data privacy service to the user device a request for approval; and

receiving, at the cloud data privacy service from the user device, a message indicating approval.

20. The computer program product according to any of the preceding claims 17 to 19, the operation further comprising:

providing, by the first data processor to a second data processor, access to at least a portion of the private data, comprising:

generating, at the cloud data privacy service based on the first data access block, a second data access block relating to a second data processor;

transmitting, from the cloud data privacy service to the first data processor, the second data access block, wherein the first data processor is configured to provide the second data access block to the second data processor;

receiving, at the cloud data privacy service from the second data processor, a request to access the at least the portion of the private data, the request comprising the second data access block; and

determining, at the cloud data privacy service, that the second data access block received from the second data processor is valid, and in response granting the second data processor at least partial access to the at least the portion of the private data.