CLAIMS

What is claimed is:

1. A privacy-preserving data risk prevention and control method, wherein the method comprises:

obtaining a processing request for target privacy data;

determining privacy data attribute information corresponding to the target privacy data, wherein the privacy data attribute information comprises information of one or more dimensions needed for controlling use of the target privacy data;

determining a control rule corresponding to the target privacy data based on the privacy data attribute information corresponding to the target privacy data, wherein the control rule corresponding to the target privacy data is constructed based on an expert knowledge base; and

controlling compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data in a process of responding to the processing request, wherein the method further comprises:

adding the target privacy data to a queue that needs to be controlled by using a predetermined privacy protection aspect; and

the obtaining a processing request for target privacy data comprises:

obtaining the processing request for the target privacy data when it is detected that a processing interface for the target privacy data receives the processing request for the target privacy data, wherein the privacy protection aspect comprises a first privacy protection subaspect and a second privacy protection subaspect, the first privacy protection subaspect is used to control processing of the target privacy data in a current terminal device, and the second privacy protection subaspect is used to control processing of outputting the target privacy data from the current terminal device;

the adding the target privacy data to a queue that needs to be controlled by using a predetermined privacy protection aspect comprises:

adding, based on the processing request for the target privacy data, the target privacy data to a queue that needs to be controlled by using the first privacy protection subaspect and/or the second privacy protection subaspect; and

the controlling compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data in a process of responding to the processing request comprises:

in the process of responding to the processing request, when it is detected, by using the first privacy protection subaspect, that the target privacy data is collected and/or consumed, controlling compliance of the use of the target privacy data based on the determined control rule corresponding

to the target privacy data;

and/or

in the process of responding to the processing request, when it is detected, by using the second privacy protection subaspect, that the target privacy data is transferred and/or copied, controlling compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data.

2. The method according to claim 1, wherein the processing request comprises one or more of a transfer request for the target privacy data, a copy request for the target privacy data, a collection request for the target privacy data, a destruction request for the target privacy data, and a consumption request for the target privacy data.

3. The method according to claim 1, wherein the privacy data attribute information comprises a data type and/or owner information of the target privacy data, and the data type comprises a location type, an environment type, and a biological recognition type.

4. The method according to claim 1, wherein the control rule corresponding to the target privacy data comprises one or more of a lifecycle control subrule, a transfer behavior control subrule, and a permission control subrule of the target privacy data.

5. The method according to claim 4, wherein the lifecycle control subrule is constructed by using information of one or more dimensions of valid duration, transfer times, and copy times of the target privacy data.

6. The method according to claim 4, wherein the transfer behavior control subrule is constructed by using information of one or more dimensions of a transfer purpose, a transfer method, and a transfer direction of the target privacy data.

7. The method according to claim 1, wherein the method further comprises:

obtaining information about the target privacy data, wherein the information about the target privacy data comprises one or more of the privacy data attribute information corresponding to the target privacy data, lifecycle information of the target privacy data, transfer behavior information of the target privacy data, and permission-related information of the target privacy data; and

determining the control rule corresponding to the target privacy data based on the information about the target privacy data.

8. A privacy-preserving data risk prevention and control apparatus, wherein the apparatus comprises:

a request obtaining module, configured to obtain a processing request for target privacy data;

an attribute obtaining module, configured to determine privacy data attribute information corresponding to the target privacy data, wherein the privacy data attribute information comprises information of one or more dimensions needed for controlling use of the target privacy data;

a control rule determining module, configured to determine a control rule corresponding to the target privacy data based on the privacy data attribute information corresponding to the target privacy data, wherein the control rule corresponding to the target privacy data is constructed based on an expert knowledge base; and

a control module, configured to control compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data in a process of responding to the processing request, wherein the apparatus further comprises:

a queue setting module, configured to add the target privacy data to a queue that needs to be controlled by using a predetermined privacy protection aspect, wherein

the request obtaining module is configured to obtain the processing request for the target privacy data when it is detected that a processing interface for the target privacy data receives the processing request for the target privacy data, wherein the privacy protection aspect comprises a first privacy protection subaspect and a second privacy protection subaspect, the first privacy protection subaspect is used to control processing of the target privacy data in a current terminal device, and the second privacy protection subaspect is used to control processing of outputting the target privacy data from the current terminal device;

the queue setting module is configured to add, based on the processing request for the target privacy data, the target privacy data to a queue that needs to be controlled by using the first privacy protection subaspect and/or the second privacy protection subaspect; and

the control module is configured to: in the process of responding to the processing request, when it is detected, by using the first privacy protection subaspect, that the target privacy data is collected and/or consumed, control compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data; and/or in the process of responding to the processing request, when it is detected, by using the second privacy protection subaspect, that the target privacy data is transferred and/or copied, control compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data.

9. The apparatus according to claim 8, wherein the control rule corresponding to the target privacy data comprises one or more of a lifecycle control subrule, a transfer behavior control subrule, and a permission control subrule of the target privacy data.

10. A privacy-preserving data risk prevention and control device, wherein the privacy-preserving data risk prevention and control device comprises:

a processor; and

a memory configured to store a computer-executable instruction, wherein when being executed, the executable instruction enables the processor to perform the following operations:

obtaining a processing request for target privacy data;

determining privacy data attribute information corresponding to the target privacy data, wherein the privacy data attribute information comprises information of one or more dimensions needed for controlling use of the target privacy data;

determining a control rule corresponding to the target privacy data based on the privacy data attribute information corresponding to the target privacy data, wherein the control rule corresponding to the target privacy data is constructed based on an expert knowledge base; and

controlling compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data in a process of responding to the processing request,

wherein the operation further comprise:

adding the target privacy data to a queue that needs to be controlled by using a predetermined privacy protection aspect; and

the obtaining a processing request for target privacy data comprises:

obtaining the processing request for the target privacy data when it is detected that a processing interface for the target privacy data receives the processing request for the target privacy data,

wherein the privacy protection aspect comprises a first privacy protection subaspect and a second privacy protection subaspect, the first privacy protection subaspect is used to control processing of the target privacy data in a current terminal device, and the second privacy protection subaspect is used to control processing of outputting the target privacy data from the current terminal device;

the adding the target privacy data to a queue that needs to be controlled by using a predetermined privacy protection aspect comprises:

adding, based on the processing request for the target privacy data, the target privacy data to a queue that needs to be controlled by using the first privacy protection subaspect and/or the second privacy protection subaspect; and

the controlling compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data in a process of responding to the processing request comprises:

in the process of responding to the processing request, when it is detected, by using the first privacy protection subaspect, that the target privacy data is collected and/or consumed, controlling compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data;

and/or

in the process of responding to the processing request, when it is detected, by using the second privacy protection subaspect, that the target privacy data is transferred and/or copied, controlling compliance of the use of the target privacy data based on the determined control rule corresponding

to the target privacy data.

11. A storage medium, wherein the storage medium is configured to store a computer-executable instruction, and the executable instruction is executed to implement the following procedure:

obtaining a processing request for target privacy data;

determining privacy data attribute information corresponding to the target privacy data, wherein the privacy data attribute information comprises information of one or more dimensions needed for controlling use of the target privacy data;

determining a control rule corresponding to the target privacy data based on the privacy data attribute information corresponding to the target privacy data, wherein the control rule corresponding to the target privacy data is constructed based on an expert knowledge base; and

controlling compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data in a process of responding to the processing request,

wherein the procedure further comprises:

adding the target privacy data to a queue that needs to be controlled by using a predetermined privacy protection aspect; and

the obtaining a processing request for target privacy data comprises:

obtaining the processing request for the target privacy data when it is detected that a processing interface for the target privacy data receives the processing request for the target privacy data,

wherein the privacy protection aspect comprises a first privacy protection subaspect and a second privacy protection subaspect, the first privacy protection subaspect is used to control processing of the target privacy data in a current terminal device, and the second privacy protection subaspect is used to control processing of outputting the target privacy data from the current terminal device;

the adding the target privacy data to a queue that needs to be controlled by using a predetermined privacy protection aspect comprises:

adding, based on the processing request for the target privacy data, the target privacy data to a queue that needs to be controlled by using the first privacy protection subaspect and/or the second privacy protection subaspect; and

the controlling compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data in a process of responding to the processing request comprises:

in the process of responding to the processing request, when it is detected, by using the first privacy protection subaspect, that the target privacy data is collected and/or consumed, controlling compliance of the use of the target privacy data based on the determined control rule corresponding

to the target privacy data;

and/or

in the process of responding to the processing request, when it is detected, by using the second privacy protection subaspect, that the target privacy data is transferred and/or copied, controlling compliance of the use of the target privacy data based on the determined control rule corresponding to the target privacy data.