(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) **CH 712 285 B1**

(51) Int. Cl.: *G06F 21/60* (2013.01)
G16H 10/60 (2018.01)

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) **PATENTSCHRIFT**

(21) Anmeldenummer: 00389/16

(22) Anmeldedatum: 21.03.2016

(43) Anmeldung veröffentlicht: 29.09.2017

(24) Patent erteilt: 30.04.2020

(45) Patentschrift veröffentlicht: 30.04.2020

(73) Inhaber:
Thomas Krech, Thundorferstrasse 194 B
8500 Frauenfeld (CH)

(72) Erfinder:
Thomas Krech, 8500 Frauenfeld (CH)

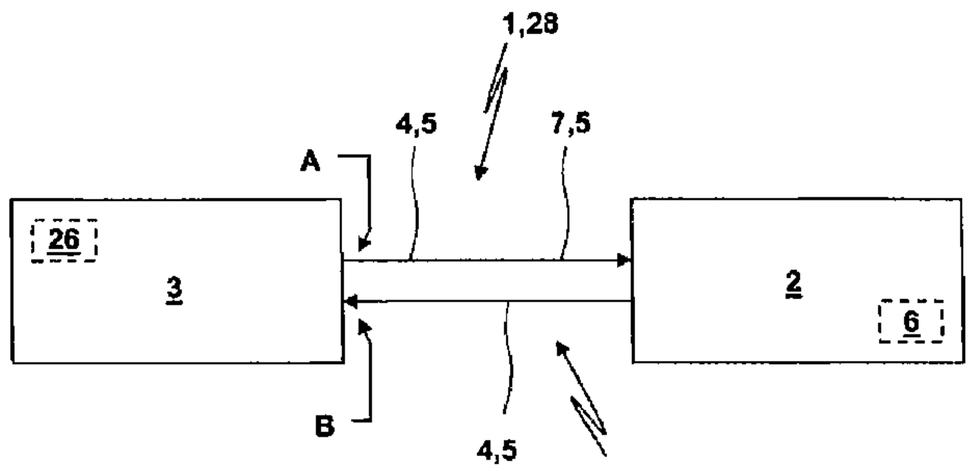
(74) Vertreter:
Riederer Hasler & Partner Patentanwälte AG,
Elestastrasse 8
7310 Bad Ragaz (CH)

(54) Daten-Netzwerk zur Umwandlung personalisierter persönlicher Daten in de-personalisierte persönliche Daten und Übermittlung der de-personalisierten Daten an einen Server.

(57) Die Erfindung betrifft ein Daten-Netzwerk mit einer Servereinrichtung (2) zur Speicherung von persönlichen Daten eines Nutzers sowie einer einem Nutzer zugeordneten Rechnereinheit (3), insbesondere einem Smartphone, Tablet-PC oder iPad sowie Desktop-PC. Die Rechnereinheit (3) und die Servereinrichtung (2) kommunizieren über ein Netzwerk (1,28), um de-personalisierte Daten auszutauschen.

Das Daten-Netzwerk entsteht dadurch, dass nur Daten über das Netzwerk geleitet und im Netzwerk gespeichert werden, die keinen direkten oder indirekten Rückschluss auf die Person zulassen; es handelt sich um sog. „de-personalisierte" Daten.

Erfindungsgemäß werden die persönlichen Daten des Nutzers bereits auf der Rechnereinheit (3) de-personalisiert mit einer Kennzeichnung (5) und an die Servereinrichtung (2) übermittelt, wo sie de-personalisiert unter der Kennzeichnung (5) gespeichert werden. Hierbei resultiert die Kennzeichnung (5) aus einer Zuordnungsvorschrift, welche ausschließlich auf der Rechnereinheit (3) abgelegt ist. Eine Personalisierung der de-personalisierten persönlichen Daten (4) in Form einer Zuordnung der de-personalisierten persönlichen Daten zu dem zugeordneten Nutzer ist auf Grundlage der auf der Servereinrichtung (2) vorhandenen de-personalisierten persönlichen Daten (4) und der Kennzeichnung (5) nicht möglich. Ferner ist eine Zuordnung während der Übermittlung der de-personalisierten Daten über das Netzwerk ebenfalls nicht möglich.



Beschreibung

TECHNISCHES GEBIET DER ERFINDUNG

[0001] Die vorliegende Erfindung betrifft Verfahren, mittels derer die Sicherheit persönlicher Daten in elektronischen Netzen und auf Servern erhöht werden kann. Dies betrifft insbesondere die Erfassung, De-Personalisierung, Re-Personalisierung, Aufbereitung und Modifikation von Daten aller Art eines Nutzers, wie Arztberichte, Befunde, Vitaldaten, Daten im Verkehr mit Banken und staatlichen sowie privaten Institutionen aller Art.

STAND DER TECHNIK

[0002] Elektronische Daten einer Person sind üblicherweise auf viele Speicherorte verteilt, angefangen von den persönlichen Daten, die beim Hausarzt, in Krankenhäusern, bei Krankenkassen, auf Smartphones - von Fitnesstrackern und Vitaldaten sowie Daten von Geräten im Sinne von Internet of things, wie beispielsweise Wasser- und Stromzählern -, über Versicherungsdaten bis hin zu Bankkontoständen und Daten bei Internet-Dienstleistern - wie Google und Facebook. Es besteht ein zunehmendes Interesse, diese Daten zusammenzuführen und zum Vorteil des Nutzers und der Allgemeinheit auszuwerten und weiterzuleiten. Die Daten eines Nutzers werden oftmals Personen oder Einrichtungen in personalisierter Form zu Verfügung gestellt und bei diesen belassen, ohne dass dies erforderlich ist.
Bei den Nutzern sowie auch von Seiten des Gesetzgebers besteht ein steigendes Interesse an der De-Personalisierung der persönlichen Daten, um einen Missbrauch der persönlichen Daten zu vermeiden. Die Bedeutung der De-Personalisierung der persönlichen Daten erhöht sich,
wenn nicht nur einzelne persönliche Daten vorliegen, sondern eine Zusammenführung sämtlicher persönlicher Daten eines Nutzers erfolgt und u. U. derartige zusammengefasste persönliche Daten zentral gespeichert werden.

[0003] Die Idee der Sammlung von persönlichen Daten zwecks Bereitstellung einer patienteneigenen mobilen Akte reift besonders in den USA immer mehr und findet beispielsweise in der iPhone - Applikation Health Chron ihren Niederschlag (vgl. https://www.linkedin.com/pulse/why-youshould-own-your-health-data-loc-pham).

[0004] Eine Datensammler-Plattform wird in den USA unter der Kennzeichnung „Physi-IQ“ entwickelt (http://www.physiq.com/markets/). Diese Datensammler-Plattform sammelt kontinuierlich Vitaldaten eines Nutzers und stellt diese dann Ärzten zur Verfügung, damit diese dann auf Grundlage der Vitaldaten proaktiv handeln zu können. Das die Datensammler-Plattform entwickelnde Unternehmen ist eine Verbindung mit dem Unternehmen Samsung eingegangen, um eine von Samsung entwickelte Datenaustausch-Plattform mit der Kennzeichnung „SAMI“ zwecks Übertragung von Sensordaten in die Cloud zu nutzen (vgl. https://developer.samsungsami.io/sami/sami-documentation/).

[0005] In Ländern wie Dänemark oder den Niederlanden werden bereits annähernd alle Patientenakten elektronisch geführt. Der Prozess der Einführung einer Digitalisierung von Patientendaten kommt hingegen bspw. in der Schweiz oder in Deutschland (http://www.healthbytes.de/eu-studie-ehealth-durchdringung-allgemeinÄrzte-deutschlandpotenzial/) nur langsam voran. Von der EU wurde die Pilot-Studie epsos (http://www.epsos.eu/home/download-area/information-on-healthcare-and-ehealth.html) lanciert mit dem Ziel, für EU-Bürger eine grenzübergreifende medizinische Versorgung auf Grundlage elektronisch gespeicherter persönliche Daten zu erproben. In der Schweiz kümmert sich innerhalb eHealth-Suisse eine interdisziplinäre Arbeitsgruppe IPAG EPD um die Strukturierung einer elektronischen Patientenakte (http://www.saez.ch/aktuelle-ausgabe/details/ipag-epd-nach-der-etappe-ist-vor-der-etappe.html). Die rechtlichen Aspekte werden in der Schweiz im Bundesgesetz über das elektronische Patientendossier geregelt (EPDG).

AUFGABE DER ERFINDUNG

[0006] Der Erfindung liegt die Aufgabe zugrunde, ein Daten-Netzwerk mit Steuerlogik für den Einsatz in einem Daten-Netzwerk (1,28) vorzuschlagen, welches hinsichtlich

- der Sicherheit der persönlichen Daten hinsichtlich eines unberechtigten Zugriffs durch Dritte,
- der De-Personalisierung von persönlichen Daten, eines Nutzers und/oder einer Vielzahl von Nutzern und/oder
- der Erzeugung personalisierter persönlicher Daten aus de-personalisierten persönlichen Daten

verbessert ist.

LÖSUNG

[0007] Die Aufgabe der Erfindung wird erfindungsgemäß mit den Merkmalen der unabhängigen Patentansprüche gelöst. Weitere bevorzugte erfindungsgemäße Ausgestaltungen sind den abhängigen Patentansprüchen zu entnehmen.

BESCHREIBUNG DER ERFINDUNG

[0008] In einem erfindungsgemäßen Daten-Netzwerk findet eine Servereinrichtung Einsatz. Bei dieser Servereinrichtung kann es sich um eine singuläre Servereinheit oder mehrere miteinander vernetzte Servereinheiten handeln. Auf der Servereinrichtung sind persönliche Daten eines Nutzers gespeichert. Bei derartigen persönlichen Daten handelt es sich bspw. um Vitaldaten eines Nutzers, wie Blutdruck, Körpertemperatur, Aktivitätsdaten, wie beispielsweise eine zurückgelegte Strecke oder eine Zahl von absolvierten Schritten oder Stufen u. ä., wobei diese Vitaldaten bspw. von sogenannten Wea-

rables wie Armbändern (http://www.aerzteblatt.de/nachrichten/62732), einer Smartphone-Fitness-Applikation (wie bspw. unter der Kennzeichnung „Endomondo“ oder wie der Health Kit von Apple oder S Health von Samsung. vertrieben), aus einer Haustechnik oder persönlichen Gebrauchsgegenständen wie einer elektrischen Zahnbürste, einem Auto oder mobilen Diagnosegeräten (http://www.aerzteblatt.de/nachrichten/62729) abgeleitet sein können. Alternativ oder kumulativ möglich ist, dass es sich bei den persönlichen Daten um Patientendaten wie bspw. Kranken- und Behandlungshistorien, Arztberichte, Überweisungsberichte, Untersuchungsbefunde wie Röntgenbilder, EKG, Laborbefunde, histologische Befunde, Bilder und Videos von Patienten (insbesondere betreffend Ergebnisse von Untersuchungsverfahren, Hautveränderungen, Schleimhautveränderungen, Wunden), Daten zur Diagnose und zur Beurteilung des Heilungsverlaufs, von Kranken- und Intensivstationen übernommene Daten, genetische Daten u. ä. handelt.

[0009] Des Weiteren verfügt das erfindungsgemäße Daten-Netzwerk über eine Rechnereinheit, die einem Nutzer zugeordnet ist. Um diesbezüglich einige nicht beschränkende Beispiele zu nennen, kann es sich bei der dem Nutzer zugeordneten Rechnereinheit um einen Computer, ein Tablet, ein Mobiltelefon, ein Smartphone, eine Smartwatch, ein Wearable oder einen PDA handeln.

[0010] Im Rahmen der Erfindung kommunizieren die Rechnereinheit und die Servereinrichtung über ein Netzwerk, um einen Austausch der persönlichen Daten zu ermöglichen. Dies kann einerseits erfolgen, um dem Nutzer einen Zugriff auf seine persönlichen Daten über die Rechnereinheit zu ermöglichen, und andererseits erfolgen, um eine Übertragung von persönlichen Daten von der Rechnereinheit zu der Servereinrichtung zwecks Abspeicherung auf der Servereinrichtung zu ermöglichen.

[0011] Erfindungsgemäß wird vorgeschlagen, dass die persönlichen Daten auf der Servereinrichtung nicht als personalisierte persönliche Daten gespeichert werden. Hierdurch soll ausgeschlossen werden, dass Dritte, welche (berechtigt oder unberechtigt) auf die Servereinrichtung zugreifen, Kenntnisse über die personalisierten persönlichen Daten erlangen. Erfindungsgemäß wird vorgeschlagen, dass die persönlichen Daten auf der Servereinrichtung ausschließlich als de-personalisierte persönliche Daten gespeichert werden. Hierbei wird unter „de-personalisierten persönlichen Daten“ jede Form der persönlichen Daten verstanden, für welche eine Zuordnung der persönlichen Daten zu der Person, welche diese persönlichen Daten betreffen, nicht möglich ist. Um diesbezüglich lediglich einige nicht beschränkende Beispiele zu nennen, können die Daten keine Bezeichnung, Kategorisierung oder eine Art „Header“ besitzen, welche einen Namen der Person oder eine sonstige für Dritte erkennbare Zuordnung zu der Person beinhaltet. Alternativ oder zusätzlich möglich ist, dass in den persönlichen Daten selbst (bspw. in einem Arztbericht oder in einem anderweitigen Dokument, einem Bild o. ä.) sämtliche persönlichen Informationen beseitigt sind.

[0012] Allerdings wäre ohne weitere erfindungsgemäße Maßnahmen ein Zugriff des Nutzers auf die persönlichen Daten nicht möglich, da ein Auffinden der de-personalisierten persönlichen Daten und deren Zuordnung zu dem Nutzer nicht mehr möglich wäre, womit die de-personalisierten persönlichen Daten „verloren“ wären. Um dies zu vermeiden, ist im Rahmen der Erfindung auf der Rechnereinheit, die dem Nutzer zugeordnet ist, eine Zuordnungsvorschrift vorhanden. Die Zuordnungsvorschrift ist hierbei an sich beliebig gestaltet, so lange diese einem Nutzer und dessen persönliche Daten eine Kennzeichnung zuweist, welche per se für Dritte nicht erkennen lässt, welchen Nutzer diese Kennzeichnung beschreibt. Um lediglich ein einfaches, die Erfindung nicht beschränkendes Beispiel zu nennen, kann die Kennzeichnung in einer einfachen Nummer bestehen, welche individuell dem Nutzer zugeordnet ist. Sind die persönlichen Daten mit dieser Nummer gekennzeichnet, kann der Nutzer bzw. die dem Nutzer zugeordnete Rechnereinheit, der oder die die Kennzeichnung in Form der Nummer über die Zuordnungsvorschrift kennt, die mit der Nummer gekennzeichneten persönlichen Daten als die seinen kennzeichnen und erkennen.

[0013] Im Rahmen der Erfindung werden die persönlichen Daten auf der Servereinrichtung sowohl mit den de-personalisierten persönlichen Daten als auch mit der genannten Kennzeichnung gespeichert. Da eine Personalisierung der de-personalisierten persönlichen Daten in Form einer Zuordnung der de-personalisierten persönlichen Daten zu dem zugeordneten Nutzer auf Grundlage der auf der Servereinrichtung vorhandenen de-personalisierten persönlichen Daten und der Kennzeichnung nicht möglich ist, ist weiterhin dem Geheimhaltungsbedürfnis der persönlichen Daten und dem Schutz gegenüber einem Missbrauch Rechnung getragen.

[0014] Die Erfindung schlägt vor, dass die Rechnereinheit, die dem Nutzer zugeordnet ist, über eine Steuerlogik, insbesondere eine Software, verfügt, mittels welcher eine Anforderung an die Servereinrichtung, dass eine Übermittlung der de-personalisierten persönlichen Daten dieses Nutzers erfolgen soll, erzeugt wird. Diese Anforderung beinhaltet die dem Nutzer zugeordnete Kennzeichnung. Empfängt die Servereinrichtung eine derartige Anforderung mit der Kennzeichnung, kann die Servereinrichtung aus vielfältigen de-personalisierten persönlichen Daten die de-personalisierten persönlichen Daten auswählen, welche der Kennzeichnung zugeordnet sind, und diese an die anfordernde Rechnereinheit übertragen, womit letztendlich dem Nutzer die diesem Nutzer zugeordneten de-personalisierten persönlichen Daten übermittelt werden, womit diese dem Nutzer zur Einsichtnahme bereitgestellt werden können.

[0015] Um die Übermittlung und das Speichern einer Vielzahl von de-personalisierten persönlichen Daten mit der Kennzeichnung, aber gleichzeitig ohne Möglichkeit des Rückschlusses auf die zugeordnete Person zu ermöglichen, schlägt die Erfindung des Weiteren vor, dass personalisierte persönliche Daten auf der Rechnereinheit des Nutzers unter Verwendung der Zuordnungsvorschrift in de-personalisierte persönliche Daten umgewandelt werden. Mit der Steuerlogik der Rechnereinheit werden dann die de-personalisierten persönlichen Daten mit der zugeordneten Kennzeichnung von der Rechner-

einheit über das Netzwerk an die Servereinrichtung übermittelt, wo diese dann ohne Möglichkeit des Rückschlusses auf den Nutzer abgespeichert werden können. Somit liegen erfindungsgemäß die persönlichen Daten in personalisierter Form lediglich auf der Rechnereinheit, aber nicht auf anderen Teilen des persönlichen Daten-Netzwerks vor. Möglich ist, diese persönlichen Daten nach der Übermittlung auf der Rechnereinheit zu löschen.

[0016] Möglich ist, dass ergänzend eine Authentifizierung des Nutzers und/oder der Rechnereinheit erforderlich ist, bevor eine Kommunikation und eine Übertragung der de-personalisierten persönlichen Daten über das persönliche Daten-Netzwerk erfolgt. Hierbei kann die Authentifizierung auch den dem Nutzer zugeordneten de-personalisierten persönlichen Daten zugeordnet sein, so dass eine Übertragung der de-personalisierten persönlichen Daten von der Servereinrichtung zu der Rechnereinheit nur dann erfolgt, wenn kumulativ eine Anforderung mit der den de-personalisierten persönlichen Daten zugeordneten Kennzeichnung erfolgt und die für diese de-personalisierten persönlichen Daten spezifische Authentifizierung vorliegt. Zur Erhöhung der Sicherheit kann es auch sein, dass zur Authentifizierung der Schlüssel einer weiteren Person notwendig ist. Dies ist beispielsweise auch dann der Fall, wenn eine Drittperson Zugriff auf die Daten oder Teile der Daten des Nutzers erhalten soll.

[0017] Ein weiterer Aspekt der Erfindung widmet sich der Problematik, dass nicht lediglich die Kennzeichnung, eine Dateibezeichnung, ein Header u. ä. einen Rückschluss auf den zugeordneten Nutzer zulassen. Vielmehr sind üblicherweise die Daten der zuvor erwähnten Art selber mit persönlichen Informationen ausgestattet. So können diese bspw. den Namen und/oder Vornamen des Nutzers, Datumsangaben, Ortsangaben, Postleitzahlen, Namen aufgesuchter Krankenhäuser, Namen von aufgesuchten Pflegeeinrichtungen, Unfallorte, Telefonnummern, Unterschriften u. ä. sonstige personenspezifische Informationen beinhalten. In weiterer Ausgestaltung der Erfindung wird vorgeschlagen, dass die dem Nutzer zugeordnete Rechnereinheit über eine Steuerlogik verfügt, mittels welcher in von den personalisierten Grunddaten umfassten Informationseinheit-Daten persönliche Informationen und solche, die auf die Person rückschliessen lassen entfernt oder umgewandelt werden können. Möglich ist hierbei, dass es sich bei den „personalisierten persönlichen Daten“ um eine umfassende Gesundheitsakte handelt, während die Informationseinheit-Daten einzelne „Blätter“ oder Teile dieser persönlichen Daten-Akte betreffen. Um lediglich einige nicht beschränkende Beispiele zu nennen, kann es sich bei den Informationseinheit-Daten um ein Bild (worunter auch eine Bildfolge in Form eines Videos verstanden wird), einen Text, eine Audio-Datei (bspw. mit einem diktierten Arztbericht, einem Echo-Kardiogramm usw.) u. ä. handeln. Möglich ist hierbei, dass die persönlichen Informationen manuell von dem Nutzer entfernt werden. Alternativ oder kumulativ möglich ist, dass die Entfernung der persönlichen Informationen automatisch erfolgt. Ebenfalls möglich ist, dass anstelle der Entfernung der persönlichen Information eine Umwandlung der persönlichen Information derart erfolgt, dass noch eine Teilinformation enthalten ist, welche dann aber einen Rückschluss auf den Nutzer nicht mehr oder nur in reduziertem Ausmaß ermöglicht.

[0018] Für eine automatische Identifikation der persönlichen Informationen zwecks Entfernung oder Umwandlung derselben gibt es vielfältige Möglichkeiten. Für einen Vorschlag der Erfindung verfügt die Rechnereinheit des Nutzers über Steuerlogik, welche eine Erkennungslogik beinhaltet. Mit der Erkennungslogik können automatisch persönliche Informationen und solche, die auf die Person rückschliessen lassen in den Informationseinheit-Daten erkannt werden. Beispielsweise kann die Erkennungslogik eine OCR-Erkennung beinhalten, welche eine in den Informationseinheit-Daten enthaltene Grafik in einen Text umwandelt. Dieser Text kann dann mit logischen Bedingungen und bekannten Bildungsgesetzen für persönliche Informationen und solche, die auf die Person rückschliessen lassen, bspw.

- mit der Suche nach Datumsangaben in vorgegebenem Datumsformat,
- mit der Suche nach Textbestandteilen, welche Namen entsprechen, wobei hinsichtlich zu berücksichtigender Namen auch auf eine diesbezügliche Datenbank zurückgegriffen werden kann u. ä.,

durchsucht werden. Führt die Erkennungslogik auf detektierte persönliche Information, kann die detektierte persönliche Information unmittelbar aus den Informationseinheit-Daten entfernt werden. Für den Fall, dass die Erkennung auf einer OCR-Erkennung basiert, muss zu diesem Zweck der Teilbereich des Bildes, welcher mit dem Textbestandteil entsprechend der OCR-Erkennung korreliert, dauerhaft entfernt werden. Möglich ist auch, dass vor einem Entfernen der persönlichen Informationen aus den Informationseinheit-Daten eine Rückfrage an den Nutzer erfolgt, welcher vor dem Entfernen eine Bestätigung geben muss.

[0019] Für ein erfindungsgemäßes Daten-Netzwerk besitzt die Rechnereinheit des Nutzers Steuerlogik, welche zumindest einen Teil der erkannten persönlichen Informationen in den Informationseinheit-Daten in verallgemeinerte persönliche Informationen und solche, die auf die Person rückschliessen lassen umwandelt. Um diesbezüglich lediglich ein nicht beschränkendes Beispiel zu nennen, kann eine persönliche Information in einer Datumsangabe mit Tag, Monat und Jahr bestehen. In diesem Fall kann die Datumsangabe zu einer verallgemeinerten persönlichen Information umgewandelt wird, welche nur noch das Jahr beinhaltet. Möglich wäre bspw. auch, dass die persönliche Information einen Wohnort oder ein Bundesland beinhaltet, während eine Umwandlung in eine verallgemeinerte persönliche Information in Form eines Bundeslands oder eines Landes oder größeren territorialen Gebiets erfolgt. Die verallgemeinerten persönlichen Informationen gewährleisten das Geheimhaltungsbedürfnis hinsichtlich der persönlichen Daten. Andererseits sind bspw. Analysen der persönlichen Daten wie die Untersuchung einer Entwicklung einer Krankheit über viele Jahre trotz Beseitigung des Tags und des Monats im Rahmen der Umwandlung möglich oder es können statistische Untersuchungen zu Krankheitshäufigkeiten unter Berücksichtigung regionaler Besonderheiten auf Grundlage der verallgemeinerten persönlichen Informationen in Form des Bundeslandes, Landes oder territorialen Gebiets vorgenommen werden. Eine weitere Möglichkeit wäre, dass eine Steuerlogik die Abstände von durch Datum gekennzeichneten Ereignissen in Zeitintervalle umwandelt. Also

beispielsweise „Erkrankungsbeginn am soundsovielten im Jahre soundsoviel und Einlieferung in die Klinik am soundsovielten im Jahre soundsoviel“ umgewandelt in „Einlieferung in die Klinik 10 Tage nach Erkrankungsbeginn“.

[0020] Für einen weiteren erfindungsgemäßen Vorschlag beinhaltet die Erkennungslogik eine Text-, Bild- oder Audioerkennungslogik. Die Steuerlogik identifiziert durch einen Abgleich erkannter Wörter, Bilder oder Audiobestandteile mit vorbestimmten Wörtern, Bildern, Audiobestandteilen oder Bildungsgesetzen persönliche Informationen und solche, die auf die Person rückschliessen lassen, wozu auch entsprechende Datenbanken mit möglichen persönlichen Informationen herangezogen werden können. Die Steuerlogik entfernt dann die derart identifizierten persönlichen Informationen aus den Informationseinheit-Daten oder wandelt diese (bspw. wie zuvor erwähnt) in verallgemeinerte persönliche Information, um.

[0021] Soll der Nutzer an der Umwandlung oder Entfernung persönlicher Informationen beteiligt werden, so kann dies für einen weiteren Vorschlag der Erfindung dadurch erfolgen, dass die Steuerlogik der Rechnereinheit des Nutzers Informationseinheit-Daten auf einer Ausgabe der Rechnereinheit, insbesondere einem Bildschirm oder einem Lautsprecher, ausgibt. Die Steuerlogik ermöglicht dann dem Nutzer, in den Informationseinheit-Daten von dem Nutzer auf Grundlage der Ausgabe identifizierte persönliche Informationen und solche, die auf die Person rückschliessen lassen zu entfernen. Um lediglich ein nicht beschränkendes Beispiel zu nennen, kann der Nutzer an einem Bildschirm einen Teilbereich der ausgegebenen Information kennzeichnen, welcher dann umgewandelt oder entfernt wird. Dies kann der Nutzer auf Grundlage der Sichtprüfung der Ausgabe vornehmen. Möglich ist auch, dass anhand eines automatisierten Verfahrens dem Benutzer nacheinander unterschiedliche identifizierte persönliche Informationen und solche, die auf die Person rückschliessen lassen angezeigt werden mit Aufforderung der Bestätigung, ob und ggf. in welchem Umfang persönliche Informationen und solche, die auf die Person rückschliessen lassen umgewandelt oder entfernt werden sollen.

[0022] Möglich ist, dass eine umgewandelte oder entfernte Information in den persönlichen Daten für immer verloren ist. Soll hingegen ermöglicht werden, dass (insbesondere nur) durch den Nutzer zu einem späteren Zeitpunkt eine Rekonstruktion der vollständigen persönlichen Daten einschl. der umgewandelten oder entfernten Information erfolgen kann, schlägt die Erfindung vor, dass mit der Steuerlogik der Rechnereinheit aus den Informationseinheit-Daten entfernte oder umgewandelte persönliche Informationen und solche, die auf die Person rückschliessen lassen gespeichert werden, was vorzugsweise ebenfalls auf der Rechnereinheit erfolgt. Vorzugsweise wird hierbei sowohl die gelöschte oder umgewandelte persönliche Information selbst als auch der Ort, an welchem sich die gelöschte oder umgewandelte persönliche Information in den Informationseinheit-Daten bzw. den persönlichen Daten befunden hat, gespeichert. Für eine zumindest teilweise Rekonstruktion der ursprünglichen persönlichen Daten oder Informationseinheit-Daten kann dann die Steuerlogik der Rechnereinheit die von der Servereinrichtung über das Netzwerk empfangenen de-personalisierten persönlichen Daten, in welchen aus Informationseinheit-Daten persönliche Informationen und solche, die auf die Person rückschliessen lassen entfernt worden sind, mit dem gespeicherten persönlichen Informationen wieder ergänzen, womit eine zumindest teilweise Vervollständigung und/oder Wiederherstellung erfolgt.

[0023] Durchaus möglich ist, dass in dem Daten-Netzwerk ausschließlich mehrere jeweils einem Nutzer zugeordnete Rechnereinheiten mit der Servereinrichtung kommunizieren. Je größer die Zahl der Nutzer und der zugeordneten Rechnereinheiten ist, desto weniger ist eine Zuordnung der de-personalisierten persönlichen Daten zu den Nutzer und Rechnereinheiten möglich. Um insbesondere zum Beginn der Befüllung der Servereinrichtung für die Übermittlung der Daten der ersten Nutzer eine Zuordnung zu diesen Nutzern zu ermöglichen, kann zumindest anfänglich die Servereinrichtung auch mit de-personalisierten persönlichen Daten von fiktiven Nutzern, welche bspw. anhand von Zufallskriterien erstellt worden sind, befüllt sein.

[0024] Möglich ist im Rahmen der Erfindung aber auch, dass in das persönliche Daten-Netzwerk weitere Einrichtungen eingebunden sind:

Für einen Vorschlag der Erfindung sind in das Daten-Netzwerk Unterstützer-Rechnereinrichtungen, insbesondere Rechnereinheiten oder Rechner-Teilnetze, integriert, welche Unterstützern für die Nutzer zugeordnet sind. Bei derartigen Unterstützern kann es sich um Gesundheitspersonal wie den Arzt oder eine behandelnde oder pflegende Person, eine Praxis oder ein Krankenhaus handeln. Andere Unterstützer, welche durch eine zugeordnete Unterstützer-Rechnereinrichtung in das persönliche Daten-Netzwerk eingebunden sein können, sind Apotheken, Versicherungen, Banken oder Forschungseinrichtungen, um nur einige zu nennen.

[0025] Soll eine Unterstützer-Rechnereinrichtung in die Lage versetzt werden, von der zentralen Servereinrichtung de-personalisierte persönlichen Daten zu erhalten, kann dies auf zwei unterschiedliche Weisen erfolgen:

a) Möglich ist, dass der Nutzer von der Rechnereinheit selbst die persönlichen Daten an die Unterstützer-Rechnereinrichtung über einen anderen Weg überträgt, bspw. über ein drahtloses oder kabelgebundenes Netzwerk.

b) Möglich wäre aber auch, dass der Nutzer die Zuordnungsvorschrift oder Kennzeichnung an die Unterstützer-Rechnereinrichtung übermittelt, womit dann der Zugriff der Unterstützer-Rechnereinrichtung auf die Servereinrichtung mit der Abfrage der de-personalisierten persönlichen Daten, die dem Nutzer, hier dem Patienten des Unterstützers gehören, erfolgen kann.

[0026] Möglich ist auch, dass das Daten-Netzwerk eine Analyse-Schnittstelle aufweist. Über die Analyse-Schnittstelle kann das persönliche Daten-Netzwerk mit einer Analyse-Rechnereinrichtung kommunizieren, in welcher eine Analyse von persönlichen Daten, bspw. zur diagnostischen Auswertung der persönlichen Daten eines Nutzers und/oder für Erhebungen oder statistische Untersuchungen der persönlichen Daten mehrerer Nutzer erfolgen kann.

[0027] Die Erfindung schlägt des Weiteren vor, dass die Unterstützer-Rechnereinrichtung, die Analyse-Rechnereinrichtung, die Servereinrichtung und/oder die dem Nutzer zugeordnete Rechnereinheit über Steuerlogik verfügt, welche aus den de-personalisierten persönlichen Daten eines Nutzer Befunde ermittelt.

[0028] Alternativ oder kumulativ möglich ist, dass die Steuerlogik automatische Nachrichten erzeugt. Um lediglich einige nicht beschränkende Beispiele zu nennen, kann aus Vitaldaten (bspw. dem Blutdruck und Puls), welche über ein Smartphone oder ein Wearable ermittelt worden sind, ein kritischer Kreislaufzustand ermittelt werden. Eine erzeugte automatische Nachricht kann bspw. eine Alarmierung des Nutzers oder einer Begleitperson des Nutzers oder eines Arztes oder eines anderweitigen Gesundheitspersonals sein. Möglich ist auch, dass als automatische Nachricht ein Hinweis auf einen turnusmäßigen Arztbesuch (bspw. über eine anstehende Impfung nach einem vorbestimmten Zeilintervall nach der vorangegangenen Impfung) erzeugt und an der Rechnereinheit des Nutzers zur Anzeige gebracht wird.

[0029] Die Erfindung schlägt auch vor, dass die Unterstützer-Rechnereinrichtung, die Analyse-Rechnereinrichtung, die Servereinrichtung und/oder die dem Nutzer zugeordnete Rechnereinrichtung über eine Erfassungseinrichtung verfügen/verfügt. Über die Erfassungseinrichtung können personalisierte oder de-personalisierte persönliche Daten erfasst werden. Möglich ist, dass die Erfassungseinrichtung eine manuelle Erfassungseinrichtung ist, über die der Nutzer persönliche Daten eingeben kann. Hierbei kann es sich um eine Tastatur handeln. Vorzugsweise ist aber die Erfassungseinrichtung als Scanner, Fotoeinrichtung, Audio-Aufnahmeeinrichtung u. ä. ausgebildet, über welche die personalisierten oder de-personalisierten persönlichen Daten erfasst werden können.

[0030] Ebenfalls möglich ist, dass als Erfassungseinrichtung an der Rechnereinheit eine Schnittstelle vorgesehen ist, wobei die Schnittstelle kabelgebunden oder kabellos ausgebildet sein kann. Über diese Schnittstelle kann die Übertragung bspw. von persönlichen Daten von einem Rechner einer Untersuchungseinrichtung des Arztes oder des Krankenhauses erfolgen oder die Kommunikation mit einem Scanner, einem Fotoapparat, einer Audio-Aufnahmeeinrichtung u. ä. erfolgen.

[0031] Alternativ oder zusätzlich kann die dem Nutzer zugeordnete Rechnereinheit über eine Schnittstelle zu einer Vitaldaten-Erfassungseinrichtung, insbesondere einem Puls-Brustgurt, einem Wearable u. ä. verfügen. Hierbei wird unter einem „Wearable" eine Rechnereinheit verstanden, welche während der Anwendung am Körper des Nutzers oder seiner Kleidung befestigt ist. Alternativ können über diese Schnittstelle bereits abgeleitete Daten empfangen werden, beispielsweise vom Apple HealthKit oder Withings.

[0032] Problematisch kann bei dem Daten-Netzwerk sein, dass zwar die persönlichen Daten zwischen der Rechnereinheit und der Servereinrichtung de-personalisiert übertragen werden, so dass aus diesen selbst unter Umständen die Zuordnung der persönlichen Daten zu dem Nutzer nicht möglich ist. Allerdings kann u. U. aus dem Übertragungspfad der de-personalisierten persönlichen Daten eine IP-Adresse, von welcher die Rechnereinheit die de-personalisierten persönlichen Daten abgesendet hat, ermittelt werden, womit letztendlich ein Rückschluss auf den Nutzer oder zumindest einen Umgebungsbereich des Nutzers möglich wäre. Soll dies vermieden werden, ist in weiterer Ausgestaltung des erfindungsgemäßen persönlichen Daten-Netzwerks zwischen die dem Nutzer zugeordnete Rechnereinheit und der Servereinrichtung eine Übertragungspfad-Trenneinrichtung zwischengeschaltet, welche die von der Rechnereinheit übertragenen de-personalisierten persönlichen Daten empfängt und unter Beseitigung von Hinweisen auf die IP-Adresse, von welcher die Übertragungspfad-Trenneinrichtung die de-personalisierten persönlichen Daten empfangen hat, dann die de-personalisierten persönlichen Daten an die Servereinrichtung überträgt. Auf diese Weise kann ein Rückschluss von den de-personalisierten persönlichen Daten auf der Servereinrichtung auf den Übertragungspfad von der Rechnereinheit unmöglich gemacht werden, womit den Geheimhaltungsinteressen des Nutzers und dem Schutz gegenüber einem Zugriff von Dritten auf die persönlichen Daten noch weiter Rechnung getragen ist.

[0033] Eine weitere Ausgestaltung der Erfindung widmet sich der Registrierung des Nutzers. Gemäß einem Vorschlag verfügt die dem Nutzer zugeordnete Rechnereinheit über Steuerlogik, die eine Telefonnummer der Rechnereinheit, insbesondere des Smartphones, aussendet. Von der für die Registrierung zuständigen Einheit, insbesondere der Servereinheit, an welche die Telefonnummer von der Rechnereinheit ausgesendet worden ist, empfängt dann die Rechnereinheit einen Code, welcher eine Authentifizierung der Rechnereinheit ermöglicht. Beispielsweise kann die Rechnereinheit bei Ausbildung derselben als Smartphone diesen Code als SMS empfangen. Erfindungsgemäß nimmt erst nach dem Empfang des Codes zur Authentifizierung der Rechnereinheit die Rechnereinheit über die Steuerlogik Daten zur Person des Nutzers auf, bei welchen es sich bspw. um Name, Geburtsdatum, Geburtsort u. ä. handeln kann. Diese Daten zur Person des Nutzers können dann in der Rechnereinheit gespeichert werden, wobei diese insbesondere nicht über das Netzwerk übertragen werden.

[0034] Grundsätzlich möglich ist, dass eine Zuordnungsvorschrift und die durch diese einem Nutzer zugeordnete Kennzeichnung sich nicht verändert. Eine weitere Erhöhung der Sicherheit des persönlichen Daten-Netzwerks kann unter Umständen herbeigeführt werden, wenn turnusgemäß oder zu bestimmten Ereignissen eine neue Zuordnungsvorschrift mit einer neuen Kennzeichnung von der Steuerlogik der Rechnereinheit ermittelt wird. Mit der ermittelten neuen Kennzeich-

nung können dann anschließend von der Rechnereinheit über das Netzwerk de-personalisierte persönliche Daten an die Servereinrichtung übermittelt werden. Unter Umständen erfolgt hierbei

- das Übertragen der de-personalisierten persönliche Daten von der Servereinrichtung an die Rechnereinheit mit der alten Kennzeichnung,
- die Ermittlung der neuen Zuordnungsvorschrift und der neuen Kennzeichnung durch die Rechnereinheit,
- das Löschen der de-personalisierten persönliche Daten mit der alten Kennzeichnung auf der Servereinrichtung und
- die Rückübertragung der de-personalisierten persönlichen Daten mit der neuen Kennzeichnung an die Servereinrichtung.

[0035] Bei den zuvor genannten Ereignissen, zu denen eine neue Zuordnungsvorschrift mit einer neuen Kennzeichnung von der Steuerlogik der Rechnereinheit ermittelt wird, kann es sich bspw. um jeden Vorgang einer Übertragung der de-personalisierten persönlichen Daten mit der (alten) Kennung von der Servereinrichtung an die Rechnereinheit und/oder die Unterstützungseinrichtung handeln. Alternativ oder zusätzlich kann als Ereignis verwendet werden, dass eine Übermittlung der Zuordnungsvorschrift an eine Unterstützungseinrichtung erfolgt ist.

[0036] Vorstellbar ist auch, dass das beschriebene Verfahren, mit dem der Nutzer den alleinigen Schlüssel zum Zugang seiner Daten hat, durch alternative Verfahren, wie Wechselcodegeräte, Papiercode oder persönliche Merkmale, wie Iriserkennung, Videosequenzen des Lidschlages, etc. oder DNA -Sequenzen ergänzt oder ersetzt werden kann.

[0037] Angestrebt sein kann, dass der Nutzer über die Rechnereinheit alleinigen personalisierten Zugriff auf seine persönlichen Daten hat. Problematisch kann dies aber u. U. bei Verlust der Rechnereinheit, Ohnmacht oder Handlungsunfähigkeit des Nutzers sein. Möglich ist, dass für die Vorsorge für derartige Fälle mittels der Steuerlogik der Rechnereinheit die Zuordnungsvorschrift an eine einer Vertrauensperson zugeordnete Rechnereinheit übermittelt wird. Bei der Vertrauensperson handelt es sich bspw. um einen Ehepartner, einen für den Nutzer im Notfall zur Entscheidung bevollmächtige Person oder eine Sicherheitsperson oder eine Person mit Treuhandfunktion, über welche bei Verlust der Rechnereinheit ein Zugriff auf die persönlichen Daten möglich bleiben soll. Der der Vertrauensperson zugeordneten Rechnereinheit kann dann ein zumindest teilweiser Zugriff auf die de-personalisierten persönlichen Daten und deren Umwandlung in personalisierte persönlichen Daten ermöglicht sein.

[0038] Grundsätzlich umfasst die Erfindung auch Ausgestaltungen, bei welchen in den persönlichen Daten sämtliche persönlichen Informationen vollständig de-personalisiert sind. Dies erschwert aber dann unter Umständen eine wissenschaftliche oder anderweitige stochastische Auswertung mit dem Ziel der Gewinnung wichtiger Erkenntnisse. Die Erfindung schlägt für eine besondere Ausgestaltung der Erfindung vor, dass die de-personalisierten persönlichen Daten hinsichtlich des Nutzers noch

- das Geburtsjahr,
- das Geschlecht des Nutzers,
- die ethnische Zugehörigkeit,
- die Zugehörigkeit zu dem Bundesland oder Kanton des Wohnorts oder dem Land des Wohnorts

beinhalten. Diese Daten können dann für eine weitergehende Auswertung der persönlichen Daten, bspw. durch wissenschaftliche Analyseinstitute, Versicherungen u. ä. genutzt werden.

[0039] Neben dem Daten-Netzwerk hat die Erfindung auch eine Software zum Gegenstand, welche mit Steuerlogik ausgestattet ist, die geeignet ist für den Einsatz und die Ausbildung eines persönlichen Daten-Netzwerks nach einem der vorhergehenden Ansprüche. Hierzu besitzt die Software insbesondere Steuerlogik, wie diese in den Patentansprüchen 1, 3 bis 9, 15, 16 beansprucht ist.

[0040] Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den Patentansprüchen. Die in der Beschreibung genannten Vorteile von Merkmalen und von Kombinationen mehrerer Merkmale sind lediglich beispielhaft und können alternativ oder kumulativ zur Wirkung kommen, ohne dass die Vorteile zwingend von erfindungsgemäßen Ausführungsformen erzielt werden müssen. Ohne dass hierdurch der Gegenstand der beigefügten Patentansprüche verändert wird, gilt hinsichtlich des Offenbarungsgehalts der ursprünglichen Anmeldungsunterlagen und des Patents Folgendes: weitere Merkmale sind den Zeichnungen - insbesondere den dargestellten Geometrien und den relativen Abmessungen mehrerer Bauteile zueinander sowie deren relativer Anordnung und Wirkverbindung - zu entnehmen.

[0041] Die in den Patentansprüchen und der Beschreibung genannten Merkmale sind bezüglich ihrer Anzahl so zu verstehen, dass genau diese Anzahl oder eine größere Anzahl als die genannte Anzahl vorhanden ist, ohne dass es einer expliziten Verwendung des Adverbs „mindestens“ bedarf. Wenn also beispielsweise von einem Element die Rede ist, ist dies so zu verstehen, dass genau ein Element, zwei Elemente oder mehr Elemente vorhanden sind. Diese Merkmale können durch andere Merkmale ergänzt werden oder die einzigen Merkmale sein, aus denen das jeweilige Erzeugnis besteht.

[0042] Die in den Patentansprüchen enthaltenen Bezugszeichen stellen keine Beschränkung des Umfangs der durch die Patentansprüche geschützten Gegenstände dar. Sie dienen lediglich dem Zweck, die Patentansprüche leichter verständlich zu machen.

KURZBESCHREIBUNG DER FIGUREN

[0043] Im Folgenden wird die Erfindung anhand in den Figuren dargestellter bevorzugter Ausführungsbeispiele weiter erläutert und beschrieben.

Fig. 1 bis 4	zeigen unterschiedliche beispielhafte Ausgestaltungen der de-personalisierten Übertragung von sensiblen Daten über ein Netzwerk, in der Regel das Internet. Dieses Netzwerk kann zusätzlich durch technische Massnahmen so ausgestaltet sein, dass geschlossene A nach B Verbindungen entstehen, z.B. als Virtual private Netzwerk (VPN) oder durch Tunnelierung.
Fig. 5	zeigt stark schematisiert Verfahrensschritte einer Steuerlogik für die Übertragung de-personalisierter Daten, wobei die Steuerlogik ein Verfahren für eine erstmalige Registrierung eines Nutzers betrifft.
Fig. 6	zeigt stark schematisiert Verfahrensschritte einer Steuerlogik für für die Übertragung de-personalisierter Daten, wobei die Steuerlogik ein Verfahren für eine Übermittlung von de-personalisierten persönlichen Daten an eine Servereinrichtung betrifft.
Fig. 7	zeigt stark schematisiert Verfahrensschritte einer Steuerlogik für die Übertragung de-personalisierter Daten, wobei die Steuerlogik ein Verfahren für die De-Personalisierung von persönliche Daten von einer Servereinrichtung betrifft.

FIGURENBESCHREIBUNG

[0044] Fig. 1 zeigt stark schematisiert ein Daten-Netzwerk 1 mit einer Servereinrichtung 2 und einer einem Nutzer oder Patienten zugeordneten Rechnereinheit 3 von einer Vielzahl von mit der Servereinrichtung 2 über ein Netzwerk 1,28 kommunizierenden, hier nicht dargestellten weiteren Rechnereinheiten. Von der Rechnereinheit 3 werden einerseits de-personalisierte persönliche Daten 4 mit zugeordneter Kennzeichnung 5 an die Servereinrichtung 2 gesendet, um unter der Kennzeichnung 5 die de-personalisierten persönlichen Daten 4 in einer Speichereinheit 6 der Servereinrichtung 2 abzuspeichern. Andererseits ist möglich, dass von der Rechnereinheit 3 eine Anforderung 7 an die Servereinrichtung 2 mit der Kennzeichnung 5 gesendet wird, die der Kennzeichnung 5 zugeordneten de-personalisierten persönlichen Daten 4 als de-personalisierte persönliche Daten 4 an die Rechnereinheit 3 zu senden. Die De-personalisierung findet durch eine Software A auf der Rechnereinheit 3 statt, die Re-personalisierung durch eine Software B auf der Rechnereinheit 3.

[0045] Um zu vermeiden, dass in der Servereinrichtung 2 über eine anfordernde IP-Adresse der Rechnereinheit 3 bereits eine Zuordnung der gespeicherten de-personalisierten persönlichen Daten 4 möglich ist, kann zwischen Servereinrichtung 2 und Rechnereinheit 3 gemäß **Fig. 2** eine Übertragungspfad-Trenneinrichtung 9 zwischengeschaltet sein. Die Übertragungspfad-Trenneinrichtung 9 empfängt die Anforderung 7 mit der Kennzeichnung 5 von der IP-Adresse der Rechnereinheit 3 und sendet diese mit der eigenen IP-Adresse ohne Hinweis auf die IP-Adresse der Rechnereinheit 3 an die Servereinrichtung 2. Die der Kennzeichnung 5 zugeordneten, in der Speichereinheit 6 gespeicherten de-personalisierten persönlichen Daten 4 werden dann von der Servereinrichtung 2 an die Übertragungspfad-Trenneinrichtung 9 übermittelt, welche dann wiederum an die nur dort vorhandene IP-Adresse der Rechnereinheit 3 die de-personalisierten persönlichen Daten 4 überträgt.

[0046] Bei ansonsten Fig. 1 entsprechender Kommunikation zwischen der Rechnereinheit 3 und der Servereinrichtung 2 verfügt gemäß **Fig. 3** das Daten-Netzwerk 1 über eine Unterstützer-Rechnereinrichtung 10, die bspw. einer Praxis, einem Krankenhaus, einer Bank oder einer Versicherung zugeordnet ist. Um dort einen Zugriff auf die persönlichen Daten zu ermöglichen, überträgt der Nutzer von der Rechnereinheit 3 de-personalisierte persönliche Daten 31 an die Unterstützer-Rechnereinrichtung 10. Gleichzeitig oder zeitlich versetzt erfolgt die Zustellung der Kennzeichnung 5, die mit den Personalien versehen ist. Diese werden bei Übereinstimmung der Kennzeichen in das Dokument als Kopfzeile eingefügt. Sofern von dem Unterstützer weitere persönliche Daten erhoben werden, kann eine Rückübertragung dieser persönlichen Daten als de-personalisierte persönliche Daten 4 mit einer zufallsgenerierten Nummer versehen (Kennzeichnung 5a) an die Rechnereinheit 3 erfolgen, womit dann auch die Übertragung dieser persönlichen Daten als de-personalisierte persönliche Daten 4 mit der zugeordneten Kennzeichnung 5a zwecks zusätzlicher Speicherung in der Servereinrichtung 2 erfolgen kann. Alternativ oder zusätzlich zu der Unterstützer-Rechnereinrichtung 10 kann eine Analyse-Rechnereinrichtung 11 Zugriff auf die de-personalisierten persönlichen Daten 33 einer Mehrzahl von Nutzern durch Kommunikation mit der Servereinrichtung 2 haben. In der Analyse-Rechnereinrichtung 11 kann dann eine Vielzahl von de-personalisierten persönlichen Daten 33 analysiert werden und das Analyseergebnis 32 der Analyse-Rechnereinrichtung 11 kann an die Servereinrichtung 2 oder andere Einrichtungen übertragen werden. Möglich ist durchaus auch, dass de-personalisierte persönliche Daten von der Unterstützer-Rechnereinrichtung 10 an eine Analyse-Rechnereinrichtung 11 übermittelt werden, womit dann von einer Analyseeinrichtung eine Analyse dieser persönlichen de-personalisierten Daten erfolgen kann. Die Analyse-Rechnereinrichtung 11 kommuniziert hierbei mit einer Analyseschnittstelle 27 der Servereinrichtung 2. Das Ergebnis der Analyse kann dann in de-personalisierter Form an die Unterstützer-Rechnereinrichtung 10 oder die Rechnereinheit 3 des Nutzers zur weiteren Verarbeitung übertragen werden.

[0047] Fig. **4** zeigt eine Ausführungsform, bei welcher (alternativ oder zusätzlich) in das Daten-Netzwerk 1,28 eine Unterstützer-Rechnereinrichtung 10 oder eine Vertrauensperson-Rechnereinheit 12 integriert ist. Um einen Austausch der dem Nutzer zugeordneten persönlichen Daten zwischen der Servereinrichtung 2 und der Unterstützer-Rechnereinrichtung 10 und/oder der Vertrauensperson-Rechnereinheit 12 zu ermöglichen, übermittelt der Nutzer über die Rechnereinheit 3 eine Zuordnungsvorschrift, insbesondere die dem Nutzer zugeordnete Kennzeichnung 5, an die Unterstützer-Rechnereinrichtung 10 und/oder die Vertrauensperson-Rechnereinheit 12. Mit dieser Zuordnungsvorschrift und ggf. weiteren übermittelten Authentifizierungen oder Passwörtern kann dann ein Datenaustausch hinsichtlich der dem Nutzer zugeordneten de-personalisierten Daten zwischen der Unterstützer-Rechnereinrichtung 10 und/oder der Vertrauensperson-Rechnereinheit 12 einerseits und der Servereinrichtung 2 andererseits erfolgen.

[0048] Als optionale weitere Möglichkeit ist in Fig. 4 dargestellt, dass die Rechnereinheit 3 über eine Schnittstelle 29 auch Vitaldaten 13 empfangen kann, welche von einem Wearable 14 oder einer Vitaldaten-Erfassungseinrichtung 30 wie einem Armband, oder einem Brustgurt oder einer Applikation des die Rechnereinheit 3 bildenden Smartphones entstammen können.

[0049] Fig. **5** zeigt beispielhaft ein Verfahren für eine erstmalige Registrierung eines Nutzers durch die diesem zugeordnete Rechnereinheit 3:

[0050] Nach dem Laden einer Applikation bspw. auf die als Smartphone ausgebildete Rechnereinheit 3 übermittelt der Nutzer in einem Verfahrensschritt 15 seine Telefonnummer an die die Registrierung durchführende Einrichtung, insbesondere die Servereinrichtung 2. In einem Verfahrensschritt 16 wird dann die Kennzeichnung 5 ermittelt, die in einem Verfahrensschritt 17 insbesondere per SMS über die zuvor übermittelte Telefonnummer an das Smartphone zurückübermittelt wird. Erst hieran anschließend erfolgt dann vom Benutzer in einem Verfahrensschritt 18 die Eingabe der persönlichen Daten. Mit dieser Registrierung ist dann das Smartphone bzw. die Rechnereinheit 3 arbeitsfähig. Insbesondere kann dann die Übertragung von de-personalisierten Daten mit der Kennzeichnung 5 oder 5a an die Servereinrichtung 2 erfolgen und/oder von der Servereinrichtung 2 können mit dem Hinweis auf die Kennzeichnung 5 oder 5a die dem Nutzer zugeordneten de-personalisierte Daten geladen werden. Weder die persönlichen Daten noch die Zuordnung zwischen der Telefonnummer und der Kennzeichnung werden auf der Servereinrichtung 2 gespeichert. Entsprechend kann verfahren werden für die Registrierung, wenn die Rechnereinheit 3 nicht als Smartphone, sondern bspw. als Desktop-Version ausgebildet ist, auf welche die Applikation geladen werden kann.

[0051] Optional kann in einem weiteren Verfahrensschritt bei der Rechnereinheit 3 angefragt werden, ob eine weitere Rechnereinheit 3 als berechtigt hinsichtlich des Nutzers registriert werden soll. Für diesen Fall wird dann die bspw. einem weiteren Smartphone zugeordnete weitere Telefonnummer von der Rechnereinheit 3 an die Servereinrichtung 2 übermittelt.

[0052] Bei den zur Person im Verfahrensschritt 18 einzugebenden Informationen handelt es sich bspw. um den Namen, Vornamen, das Geburtsdatum, das Geschlecht, die ethnische Zugehörigkeit, das Gewicht, die Größe, die Straße, den Wohnort, das Land, die E-Mail-Adresse, die Mobiltelefonnummer, eine Personalausweisnummer u. ä.

[0053] Unter Umständen kann in einem zusätzlichen Verfahrensschritt geprüft werden, ob es sich bei dem Anmelder um eine natürliche Person handelt. Weiterhin kann eine Verifizierung der Angaben zur Person durch Zugriff auf eine entsprechende Datenbank erfolgen. Es ist auch möglich, dass während der Registrierung eine Einverständniserklärung mit den AGB gefordert wird. Hierbei können die AGB auch beinhalten, dass der Nutzer zustimmt, dass die de-personalisierten Daten des Patienten wissenschaftlich ausgewertet und/oder finanziell verwertet werden.

[0054] Fig. **6** zeigt die Übermittlung von de-personalisierten persönlichen Daten an die Servereinrichtung 2 zwecks Speicherung derselben:

Die zunächst genannten Verfahrensschritte werden entweder von der Rechnereinheit 3, welche mit der Servereinrichtung 2 kommunizieren kann (Fig. 1), oder der Unterstützer-Rechnereinrichtung 10 oder der Vertrauensperson-Rechnereinheit 12, welche mit der Servereinrichtung 2 kommunizieren kann (Fig. 4), durchgeführt.

[0055] In einem Verfahrensschritt 19 werden zunächst persönliche Daten gewonnen. Dies kann durch Empfangen der persönlichen Daten von einem Untersuchungsgerät, von der Unterstützer-Rechnereinrichtung 10 oder durch Erfassung eines Arztberichts u. ä. über eine Erfassungseinrichtung 26 erfolgen. In einem anschließenden Verfahrensschritt 20 werden dann persönliche Informationen und solche, die auf die Person rückschliessen lassen aus Informationseinheit-Daten, also bspw. dem Arztbericht, dem Röntgenbild u. ä. entfernt. Hieran anschließend wird im Verfahrensschritt 21 das Datenpaket, welches sowohl die de-personalisierten Daten als auch die zugehörige Kennzeichnung beinhaltet, an die Servereinrichtung 2 übermittelt. Die Servereinrichtung 2 speichert dann im Verfahrensschritt 22 unter der Kennzeichnung 5 die empfangenen de-personalisierten Daten in der Speichereinheit 6 ab.

[0056] Fig. **7** zeigt das Verfahren für das Laden von de-personalisierten Daten von der Servereinrichtung 2 in die Rechnereinheit 3 (Fig. 1) bzw. in die Unterstützer-Rechnereinrichtung 10 oder Vertrauensperson-Rechnereinheit 12 (vgl. Fig. 4):

In einem Verfahrensschritt 23 übermittelt die Rechnereinheit 3 (bzw. die Unterstützer-Rechnereinrichtung 10 oder die Vertrauensperson-Rechnereinheit 12) eine Anforderung 7 mit der Kennzeichnung 5 an die Servereinrichtung 2. Die Servereinrichtung 2 lädt in einem Verfahrensschritt 24 die der Kennzeichnung 5 zugeordneten de-personalisierten Daten aus der Speichereinheit 6. Die de-personalisierten Daten werden dann in dem Verfahrensschritt 25 an die Rechnereinheit 3 (bzw. die Unterstützer-Rechnereinheit 10 oder die Vertrauensperson-Rechnereinheit 12) übertragen, wo sie re-personalisiert werden, indem z.B. in einer Kopfzeile (Header) die Daten zur Person aufgeführt werden.

[0057] Die Servereinrichtung 2 kann auf der Speichereinheit 6 die de-personalisierten Daten vieler Nutzer zunächst nach der jeweiligen Kennzeichnung 5 ablegen. Diese mehrere Nutzer-Daten umfassende Ablage ist in den Abbildungen als 33 dargestellt. Eine Extrahierung von Suchwörtern zur Ermöglichung einer Suchfunktion für eine Analyse der de-personalisierten Daten mehrerer Nutzer (33) ist ebenfalls möglich. Eine Kategorisierung der de-personalisierten Daten zu einem Nutzer kann bspw. nach Art der Informationseinheit-Daten erfolgen. So kann bspw. eine Klassifizierung zwischen Untersuchungsbefunden, Arztbriefen, Entlassungsberichten erfolgen. Ebenfalls möglich ist, dass die Zusammenfassung von Informationseinheit-Daten oder Kennzeichnung derselben je nach durchführendem Institut der einzelnen Untersuchungen und Arztberichte erfolgt. Alternativ oder zusätzlich möglich ist die Kategorisierung der Informationseinheit-Daten je nach Erkrankung oder betroffenem Körperteil oder dem medizinischen Fachgebiet. Möglich ist, dass Informationseinheit-Daten unterschiedlicher Kategorien einzeln dem Nutzer oder einem Unterstützer bereitgestellt werden.

[0058] Eine Applikation der Rechnereinheit 3 kann eine Suchfunktion beinhalten, um ein einfaches Wiederauffinden von Informationen zu ermöglichen.

[0059] Beispiele für Wearables 14, welche im Rahmen der Erfindung in dem Daten-Netzwerk 1 eingesetzt werden können, sind bspw. Auf der Internet-Seite (http://www.emdt.co.uk/ daily-buzzl5-wearables-could-transform-healthcare) angeführt. Beispiele hierfür sind

- „Google lens“ für eine Blutzuckermessung,
- „WearSens“ für die Messung der Nahrungsaufnahme (vgl. http://www.medicaldaily.com/ucla-engineers-develop-wearsens-food-diary-you-canwear-around-your-neck-324508),
- Google smart pill, um Krebs zu entdecken (vgl. http://mobihealthnews.com/37730/google-x-developing-cancer-scanning-pill-thattransmits-to-a-wearable-sensor/),
- Wearable-Sensoren für die kontinuierliche Messung von Körperflüssigkeiten (vgl. http://www.emdt.co.uk/daily-buzz/higher-powered-wearable-sensors) sowie
- Sensoren für eine kontinuierliche EKG-Messung (vgl. http://internetmedicine.com/ irhythm/).

[0060] Eine in das Daten-Netzwerk 1 integrierte Analyseeinrichtung kann eine Vielzahl von de-personalisierten Daten eines Patienten oder mehrerer Patienten auswerten, wobei eine zusätzliche Validierung und Freigabe unter ärztlichen Gesichtspunkten erfolgen kann. Die aus der Analyse resultierenden Analyseergebnisse oder die generierten Daten-Extrakte können insbesondere die folgenden Informationen und Daten beinhalten:

- einen elektronischen Arztbrief (vgl. http://www.aerzteblatt.de/archiv/167716/ Elektronischer-Arztbrief-Arztnetze-fuer-die-Erprobung-gesucht),
- Austrittsberichte, Kontoauszüge
- Diagnoselisten, Ausgabenlisten nach Kategorien als Bank-Kontoauszüge
- Überweisungsberichte, Zahlungstransfers, Schaden-Rapporte
- Risikoanalysen,
- Zusammenfassungen zu bestimmten Fragestellungen,
- Erinnerungen und Aufforderungen zum Arztbesuch, zur Impfung, zur Krebsvorsorgeuntersuchung, zur Tabletteneinnahme etc., zu Daueraufträgen im Bank-Zahlungsverkehr
- Auswertungen und Beurteilungen von medizinischen Bildern (Röntgenbilder, Blutbilder, Hautveränderungen),
- Alarmierung des Gesundheitspersonals bei kritischen Vitaldaten bei Patienten auf der Intensivstation, auf der Abteilung, im Pflegeheim oder zu Hause beim betreuten Wohnen sowie
- Auswertungen für die pharmazeutische Industrie, für Versicherungen und zu wissenschaflichen Zwecken.

[0061] Auf der Rechnereinheit 3 erfolgt, insbesondere mittels einer Smartphone-Applikation, die Registrierung, die temporäre Speicherung der persönlichen Daten, die Beschaffung und das Einlesen neuer persönlicher Daten, die De-personalisierung der persönlichen Daten, die Generierung von Kennzeichnungen zur Verwendung mit de-personalisierten Datenpaketen und die Herstellung der Verbindung zur Servereinrichtung 2 mit dem dann folgenden Upload.

[0062] Hingegen erfolgt auf der Servereinrichtung 2 die Verwaltung der de-personalisierten persönlichen Daten mit der zugeordneten Kennzeichnung und die Zugriffsverwaltung für die Nutzer sowie Analyseeinrichtungen u. ä.

[0063] Eine Applikation einer als Smartphone ausgebildeten Rechnereinrichtung 3 kann bspw. eine Menüoberfläche beinhalten, welche die Menüpunkte

- Login zur Ermöglichung des Logins mit einer Benutzerkennung und einem Passwort,
- „meine persönlichen Daten online“,
- „meine nächsten Termine“,

– „Persönliche Daten scannen“,
– „Persönliche Daten importieren“,
– „Persönliche Daten aufbereiten“,
– „Rezept anfordern“,
– „Laboruntersuchung durchführen“,
– „Arzttermin buchen“,
– „Chat“,
– „Einstellungen“ und/oder
– „Favoriten verwalten“

beinhaltet, und die zugeordneten Funktionen ausführen.

[0064] Eine Übersendung von de-personalisierter Daten über das Daten-Netzwerk 1,28 erfolgt insbesondere als Metadaten nach dem Standard IHE. Möglich ist, dass zur Re-Personalisierung anstelle des (Wieder-)Einsetzen der Patientendaten in das Dokument die Kennzeichnung 5 als Kopfzeile oder Header in die Dokumente eingefügt wird, welche sich über die Zuordnungsvorschrift von dem Nutzer mit dessen Personal-Daten verknüpfen lässt. Der Download und der Upload der de-personalisierten Daten erfolgt über eine verschlüsselte Verbindung. Eine Verschlüsselung der de-personalisierten persönlichen Daten kann zusätzlich entsprechend den üblichen bekannten Verschlüsselungstechnologien erfolgen.

[0065] Möglich ist, dass eine Zugriffsverwaltung für Dritte wie Vertrauenspersonen oder Analyseeinrichtungen durch ein Protokoll mit der Kennzeichnung „OAuth“ erfolgt, wie dieses in der einschlägigen Fachliteratur und unter https://de.wikipedia.org/wiki/OAuth beschrieben ist. Auf welche Bestandteile der de-personalisierten Daten Dritte zugreifen können, kann der Nutzer individuell aufgrund hinterlegter Profile bestimmen und durch die Applikation auf der Rechnereinheit 3 oder der Servereinrichtung 2 steuern.

[0066] Möglich ist, dass der Nutzer beim Anlegen seines Profils das Einverständnis geben muss, dass eine Weitergabe der persönlichen Daten an Dritte, Bevollmächtigte oder eine Vertrauensperson unter Umständen in letzter Instanz von einer Treuhandstelle freigegeben werden kann. Ein Datenzugriff durch einen Stellvertreter kommt insbesondere dann in Frage, wenn der Nutzer bewusstlos ist, bevormundet wird, verstorben ist oder die Rechnereinheit 3, welche ausschließlich die Zuordnungsvorschrift beinhaltet, verlorengegangen ist.

[0067] Möglich ist, dass im Rahmen der Erfindung ein auf der Internet-Seite https://validic.com/api beschriebenes Verfahren Einsatz findet.

[0068] Für die Beseitigung persönlicher Informationen kann ein Dokument, wie ein Arztbrief oder ein Röntgenbild, zunächst vollständig „geschwärzt“ oder gelöscht werden, wonach dann der Benutzer über eine Art Wischfunktion „selektiv“ einzelne Bestandteile dieses Dokuments wieder reaktivieren kann. Umgekehrt kann der Nutzer noch nicht „geschwärzte“ Stellen in seinem Dokument, die auf seine Person schliessen lassen, durch eine Wischfunktion selbst schwärzen.

BEZUGSZEICHENLISTE

[0069]

A	Programm zur De-Personalisierung (De-Identifikation) der Daten in elektronischer oder handgeschriebener Form.
B	Programm zur Re-Personalisierung (Re-Identifikation) der Daten durch Wiederherstellung des Originaldokumentes oder durch Einfügen einer Markierung (Header) mit den Personen-Stammdaten, wie Name, Vorname, Geschlecht, Geburtsdatum.
C	Programm(e) zur Datenanalyse
1	Persönliches geschlossenes Datennetzwerk, z.B. tunneliert oder VPN, über welches sensible Daten aller Art - beispielsweise Gesundheitsdaten und Bankdaten - in personalisierter oder de-personalisierter Form ausgetauscht werden können.
2	Servereinrichtung (vom Nutzer entfernt und über ein Netzwerk verbundene Einrichtung zur Speicherung und Verwaltung von Daten)
3	Persönliche Rechnereinheit (vom Nutzer kontrollierte elektronische Einrichtung, wie z.B. Smartphone, Tablett-PC, Desktop-PC, zur Aufnahme, Verarbeitung, Verwaltung und De-Personalisierung von Daten)
4	Oe-personalisierte persönliche Daten (Daten, die ohne Schlüssel nicht mehr einer Person zugeordnet werden können).
5	Kennzeichnung (der de-personalisierten Daten, die nur mit einem Schlüssel wieder einer Person zugeordnet werden können).
5a	Zufallsgenerierte Kennzeichnung
6	Speichereinheit (technische Einrichtung zur Speicherung de-personalisierter Daten)
7	Anforderung (elektronische Anfrage bzw. elektronischer Auftrag)
8	personalisierte persönliche Daten in elektronischer Form oder anderer Form, wie z.B. auf Papier.
8a	Re-personalisierte persönliche Daten in Form des Originals oder mit einem Kopf (Header) versehen, der die Angaben zur Person enthält.
9	Übertragungspfad-Trenneinrichtung (Einrichtung, die eine Rückverfolgung der Daten zur Verschlüsselung verunmöglicht).

10 Unterstützer-Rechnereinrichtung (Rechnereinrichtung einer den Nutzer unterstützenden Institution, wie beispielsweise Krankenhaus, Arzt oder Bank bzw. Versicherung).
11 Analyse-Rechnereinrichtung (Rechnereinrichtung zur Analyse und Auswertung von
12 Daten, wie Vitaldaten, Bankdaten, Gesundheitsdaten etc. mit dem primären Ziel, die Auswertungen und Erkenntnisse dem Nutzer zur Kenntnis zu bringen und dem sekundären Ziel, neue Kenntnisse von allgemeinem Interesse zu gewinnen). Vertrauensperson-Rechnereinheit (Rechnereinheit einer Person mit treuhänderischer Funktion)
13 Vitaldaten (Messdaten, wie Gewicht, Puls, Blutdruck, Blutzucker, etc.)
14 Wearable (Kleidungsstück, Patch oder Accessoire, wie z.B. Armband, mit eingebauten Sensoren zur Messung von Vitaldaten und Ereignissen, wie z.B. Medikamenten-Einnahme oder Registrierung von Waren beim Einkaufen)
15 Verfahrensschritt
16 Verfahrensschritt
17 Verfahrensschritt
18 Verfahrensschritt
19 Verfahrensschritt
20 Verfahrensschritt
21 Verfahrensschritt
22 Verfahrensschritt
23 Verfahrensschritt
24 Verfahrensschritt
25 Verfahrensschritt
26 Erfassungseinrichtung
27 Analyseschnittstelle (Schnittstelle zwischen gespeicherten de-personalisierten Daten und Einrichtung zur Verarbeitung, Speicherung und Weitergabe von Daten)
28 Persönliches öffentliches Netzwerk, Internet
29 Schnittstelle
30 Erfassungseinrichtung von Daten aus Wearables, Handhelds, Waagen, elektronischen Einrichtungen in Fahrzeugen, wie Steuerrad und Kameras sowie in Immobilien, wie Strom- und Wasserzählern.
31 personalisierte persönliche Daten
32 Analyseergebnis
33 De-personalisierte Daten einer Vielzahl von Nutzern

Patentansprüche

1. Daten-Netzwerk mit
a) einer Servereinrichtung (2), auf welcher persönliche Daten eines Nutzers gespeichert sind, und
b) einer einem Nutzer zugeordneten Rechnereinheit (3),
c) wobei die Rechnereinheit (3) und die Servereinrichtung (2) über ein Netzwerk (1,28) zum Austausch der persönlichen Daten miteinander kommunizieren, **dadurch gekennzeichnet**, dass
d) auf der dem Nutzer zugeordneten Rechnereinheit (3) eine Zuordnungsvorschrift vorhanden ist, welche dem Nutzer und dessen de-personalisierten persönlichen Daten eine Kennzeichnung (5) zuweist,
e) die persönlichen Daten auf der Servereinrichtung (2) ausschließlich als de-personalisierte persönliche Daten (4) mit der Kennzeichnung gespeichert sind, wobei eine Personalisierung der de-personalisierten persönlichen Daten (4) in Form einer Zuordnung der de-personalisierten persönlichen Daten zu dem zugeordneten Nutzer auf Grundlage der auf der Servereinrichtung (2) vorhandenen de-personalisierten persönlichen Daten (4) und der Kennzeichnung (5) nicht möglich ist,
f) die dem Nutzer zugeordnete Rechnereinheit (3) über Steuerlogik verfügt, welche
a) eine Anforderung (7) an die Servereinrichtung (2) hinsichtlich der Übermittlung der de-personalisierten persönlichen Daten (4) erzeugt, wobei die Anforderung die dem Nutzer zugeordnete Kennzeichnung (5) beinhaltet, und die auf die Anforderung von der Servereinrichtung (2) über das Netzwerk (28) an die Rechnereinheit (3) übermittelten de-personalisierten persönlichen Daten (4), welchen die Kennzeichnung (5) zugeordnet ist, empfängt und/oder
b) personalisierte persönliche Daten auf der Rechnereinheit (3) unter Verwendung der Zuordnungsvorschrift in de-personalisierte persönliche Daten (4) mit zugeordneter Kennzeichnung (5) umwandelt und dann die da-personalisierten persönlichen Daten (4) mit der zugeordneten Kennzeichnung (5) von der Rechnereinheit (3) über das Netzwerk (1,28) an die Servereinrichtung (2) übermittelt.

2. Daten-Netzwerk nach Anspruch 1, **dadurch gekennzeichnet**, dass die dem Nutzer zugeordnete Rechnereinheit (3) ein Computer, ein Tablet, ein Mobiltelefon, ein Smartphone, eine Smartwatch, ein Wearable oder ein PDA ist.

3. Daten-Netzwerk nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, dass die dem Nutzer zugeordnete Rechnereinheit (3) über Steuerlogik verfügt, mittels welcher in von den personalisierten persönlichen Daten umfassten Informationseinheit-Daten persönliche Informationen und solche, die auf die Person rückschliessen lassen,
a) automatisch und/oder
b) manuell von dem Nutzer

entfernt oder umgewandelt werden können.

4. Daten-Netzwerk nach Anspruch 3, **dadurch gekennzeichnet**, dass die dem Nutzer zugeordnete Rechnereinheit (3) über eine Steuerlogik verfügt, welche eine Erkennungslogik beinhaltet, mittels welcher automatisch persönliche Informationen und solche, die auf die Person rückschliessen lassen, in den Informationseinheit-Daten erkannt und aus den Informationseinheit-Daten entfernt werden können.

5. Daten-Netzwerk nach Anspruch 3 oder 4, **dadurch gekennzeichnet**, dass die dem Nutzer zugeordnete Rechnereinheit (3) über eine Steuerlogik verfügt, welche persönliche Informationen und solche, die auf die Person rückschliessen lassen in verallgemeinerte persönliche Informationen umwandelt.

6. Daten-Netzwerk nach einem der Ansprüche 4 oder 5, **dadurch gekennzeichnet**, dass
a) die Erkennungslogik eine Text-, Bild- oder Audioerkennungslogik beinhaltet,
b) die Steuerlogik durch einen Abgleich erkannter Wörter, Bilder oder Audiobestandteile mit vorbestimmten Wörtern, Bildern, Audiobestandteilen oder Bildungsgesetzen persönliche Informationen und solche, die auf die Person rückschliessen lassen identifiziert und
c) die Steuerlogik die identifizierten persönlichen Informationen aus den Informationseinheit-Daten entfernt oder in verallgemeinerte persönliche Informationen umwandelt.

7. Daten-Netzwerk nach einem der Ansprüche 3 bis 6, **dadurch gekennzeichnet**, dass die dem Nutzer zugeordnete Rechnereinheit (3) über Steuerlogik verfügt,
a) welche die Informationseinheit-Daten auf einer Ausgabe der Rechnereinheit (3) ausgibt, und
b) welche es dem Nutzer ermöglicht, in den Informationseinheit-Daten auf Grundlage der Ausgabe identifizierte persönliche Informationen und solche, die auf die Person rückschliessen lassen zu entfernen oder in verallgemeinerte persönliche Informationen umzuwandeln.

8. Daten-Netzwerk nach einem der Ansprüche 3 bis 7, **dadurch gekennzeichnet**, dass die dem Nutzer zugeordnete Rechnereinheit (3) über Steuerlogik verfügt,
a) welche aus den Informationseinheit-Daten entfernte oder in verallgemeinerte persönliche Informationen umgewandelte persönliche Informationen speichert und
b) welche aus
ba) den von der Servereinrichtung (2) über das Netzwerk (1,28) empfangenen de-personalisierten persönlichen Daten (4), in welchen aus Informationseinheit-Daten persönliche Informationen und solche, die auf die Person rückschliessen lassen entfernt oder in verallgemeinerte persönliche Informationen umgewandelt worden sind, und
bb) den gespeicherten persönlichen Informationen
eine zumindest teilweise Rekonstruktion der ursprünglichen Informationseinheit-Daten mit den persönlichen Informationen vornimmt.

9. Daten-Netzwerk nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass die dem Nutzer zugeordnete Rechnereinheit (3) über Steuerlogik verfügt, welche
a) eine Übermittlung personalisierter persönlicher Daten (31) und/oder
b) eine Übermittlung der Zuordnungsvorschrift
an eine Unterstützer-Rechnereinrichtung (10) ermöglicht.

10. Daten-Netzwerk nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass die Servereinrichtung (2) über eine Analyse-Schnittstelle (27) mit einer Analyse-Rechnereinrichtung (11) verbunden ist.

11. Daten-Netzwerk nach Anspruch 10, **dadurch gekennzeichnet**, dass die Unterstützer-Rechnereinrichtung (12), die Analyse-Rechnereinrichtung (11), die Servereinrichtung (2) und/oder die dem Nutzer zugeordnete Rechnereinheit (3) über Steuerlogik verfügt, welche aus den de-personalisierte persönliche Daten (4) eines Nutzers Befunde ermittelt und/oder automatische Nachrichten erzeugt.

12. Daten-Netzwerk nach Anspruch 10 oder 11, **dadurch gekennzeichnet**, dass die Unterstützer-Rechnereinrichtung (10), die Analyse-Rechnereinrichtung (11), die Servereinrichtung (2) und/oder die dem Nutzer zugeordnete Rechnereinheit (3) über eine Erfassungseinrichtung (26) verfügt, welche personalisierte oder de-personalisierte persönliche Daten erfassen kann.

13. Daten-Netzwerk nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass die dem Nutzer zugeordnete Rechnereinheit (3) über eine Schnittstelle (29) zu einer Vitaldaten-Erfassungseinrichtung (30) verfügt.

14. Daten-Netzwerk nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass zwischen die dem Nutzer zugeordnete Rechnereinheit (3) und der Servereinrichtung (2) eine Übertragungspfad-Trenneinrichtung (9) zwischengeschaltet ist, welche die von der Rechnereinheit (3) übertragenen de-personalisierten persönlichen Daten (4) an die Servereinrichtung (2) überträgt und einen Rückschluss von de-personalisierten persönlichen Daten (4) auf der Servereinrichtung (2) auf den Übertragungspfad von der Rechnereinheit (3) unmöglich macht.

15. Daten-Netzwerk nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass für eine Registrierung des Nutzers die dem Nutzer zugeordnete Rechnereinheit (3) über Steuerlogik verfügt, welche
a) eine Telefonnummer der Rechnereinheit (3) aussendet,

b) einen Code zur Authentifizierung der Rechnereinheit (3) empfängt und
c) erst nach dem Empfang des Codes zur Authentifizierung der Rechnereinheit (3) Daten zur Person des Nutzers aufnimmt und diese dann in der Rechnereinheit (3) speichert.

16. Daten-Netzwerk nach einem der Ansprüche 9 bis 15, **dadurch gekennzeichnet**, dass die dem Nutzer zugeordnete Rechnereinheit (3) über Steuerlogik verfügt,
a) welche
aa) nach dem Übertragen der de-personalisierten persönlichen Daten (4) von der Servereinrichtung (2) an die Rechnereinheit (3) und/oder die Unterstützer-Rechnereinrichtung (10) und/oder
ab) nach einer Übermittlung der Zuordnungsvorschrift oder Kennzeichnung (5) an eine Unterstützer-Rechnereinrichtung (10)
eine neue Zuordnungsvorschrift mit einer neuen Kennzeichnung ermittelt,
c) welche dann die de-personalisierten persönlichen Daten (4) mit der neuen Kennzeichnung (5) von der Rechnereinheit (3) über das Netzwerk (1,28) an die Servereinrichtung (2) übermittelt.

17. Daten-Netzwerk nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, dass die Rechnereinheit (3) die Zuordnungsvorschrift an eine einer Vertrauensperson zugeordnete Vertrauensperson-Rechnereinheit (12) übermittelt, sodass der Vertrauensperson-Rechnereinheit (12) ein zumindest teilweiser Zugriff auf die de-personalisierten persönlichen Daten und deren Umwandlung in personalisierte persönliche Daten ermöglichtist.

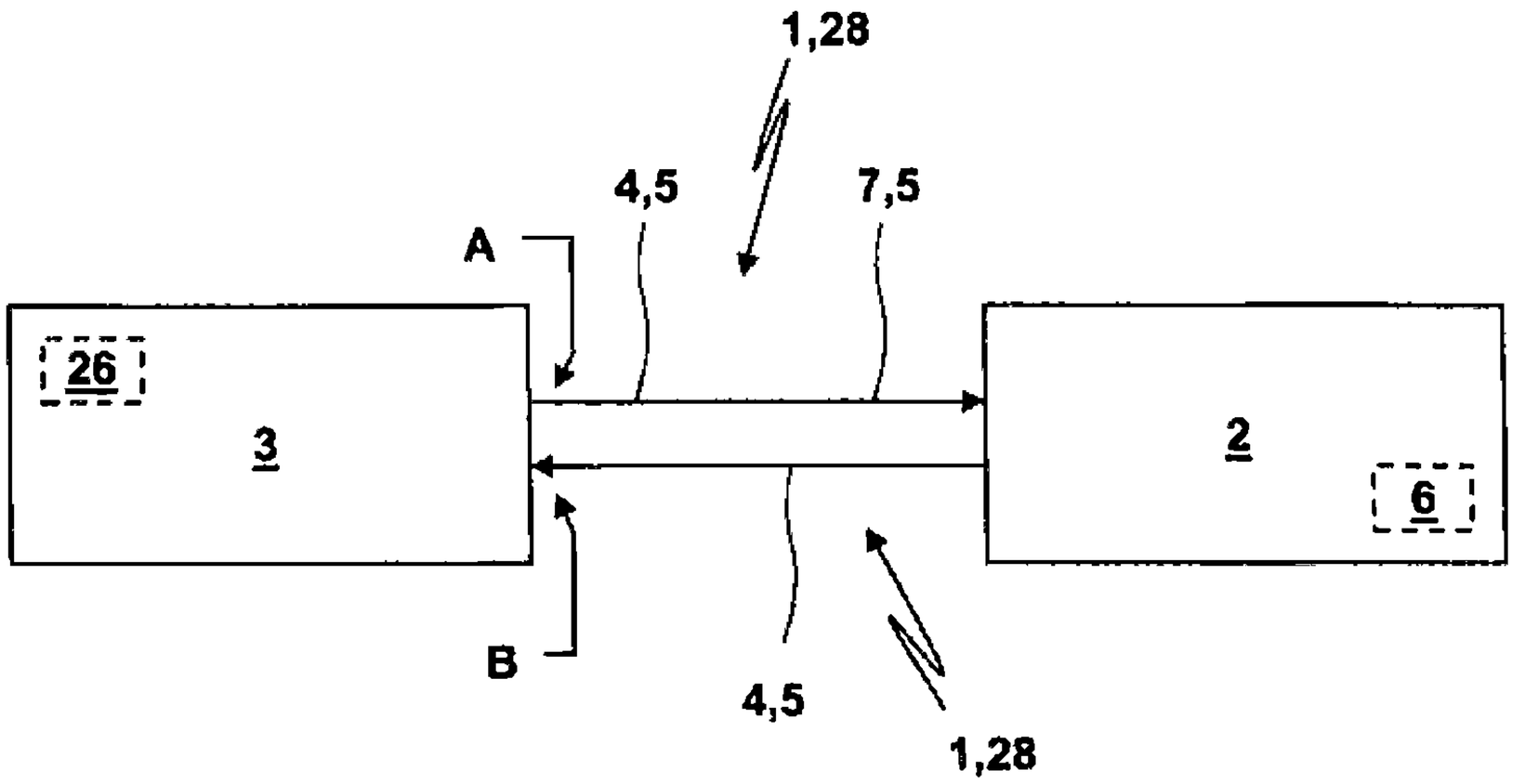


Fig. 1

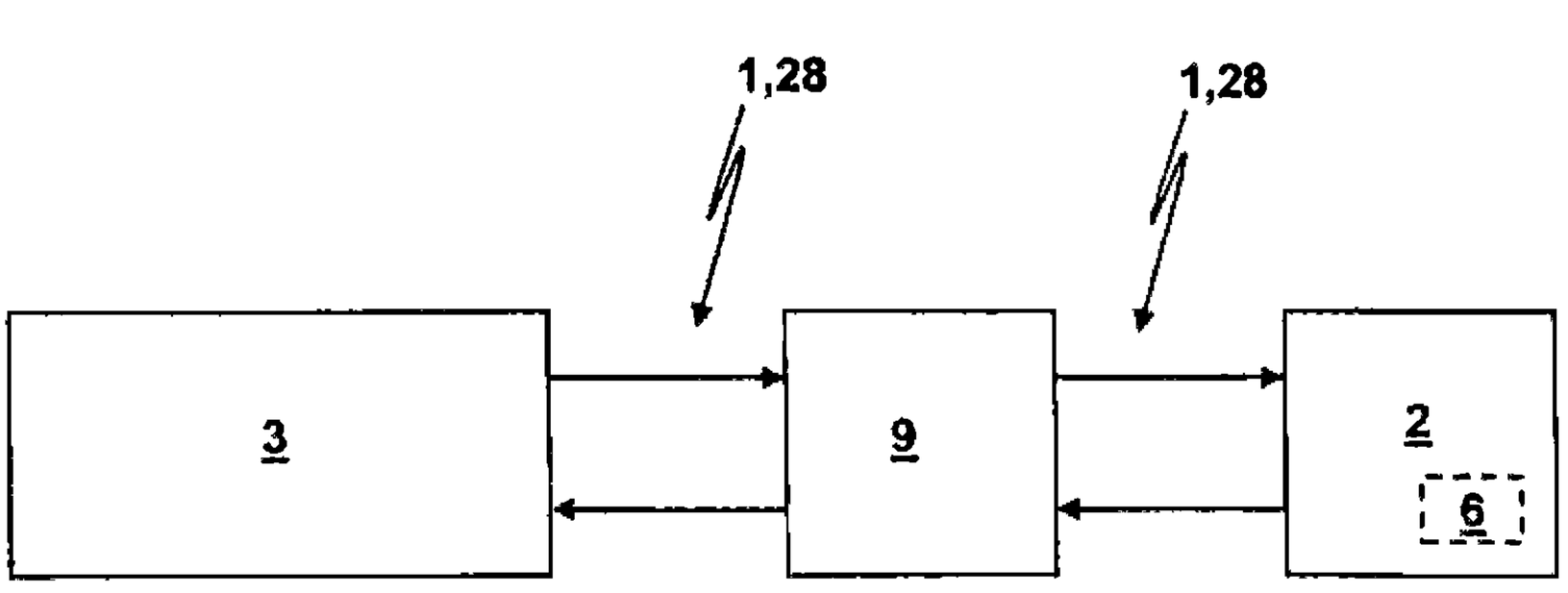


Fig. 2

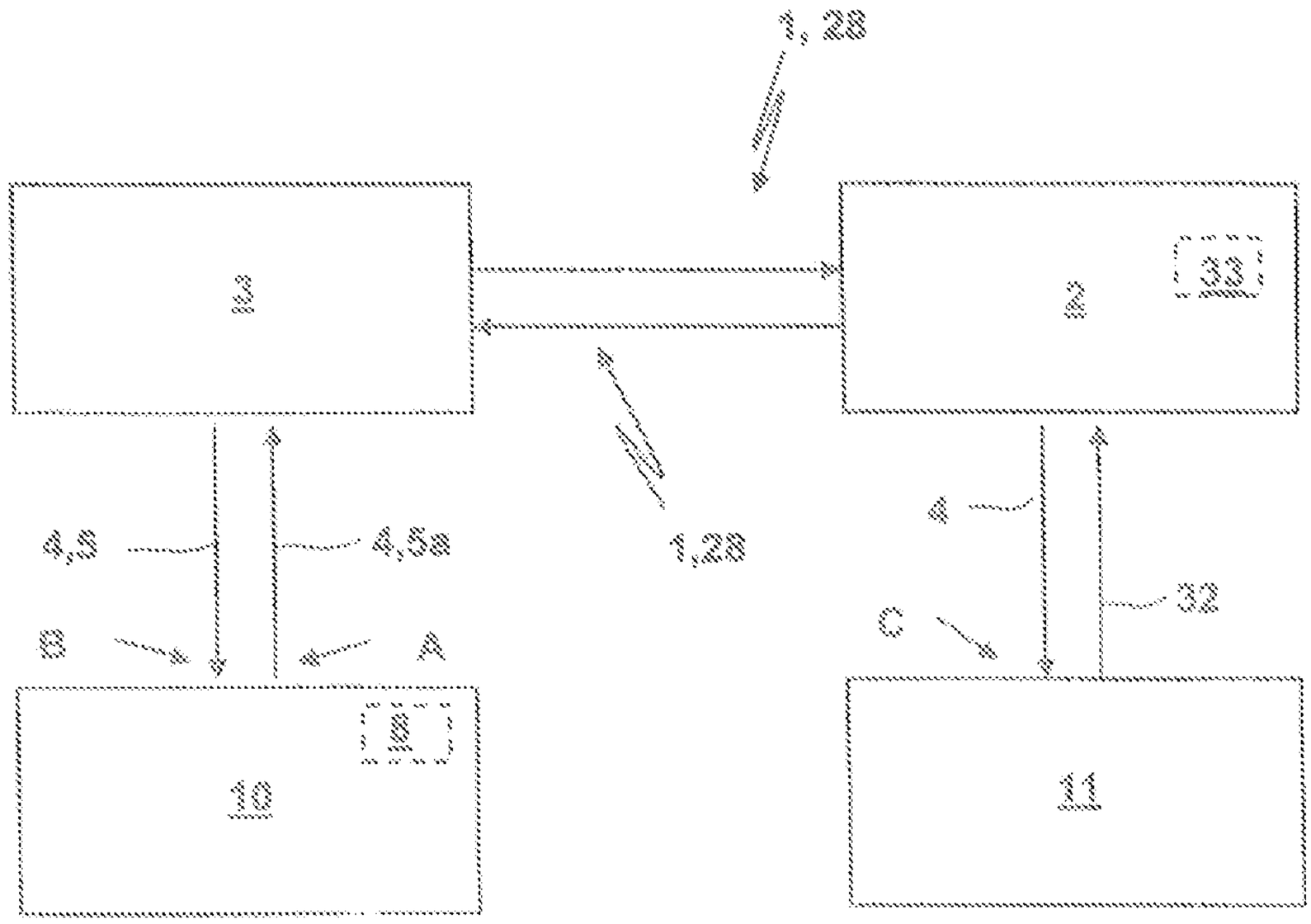

1,28
3
2
38
4,5
4,5a
1,28
4
32
B
A
C
38
10
11

Fig. 3

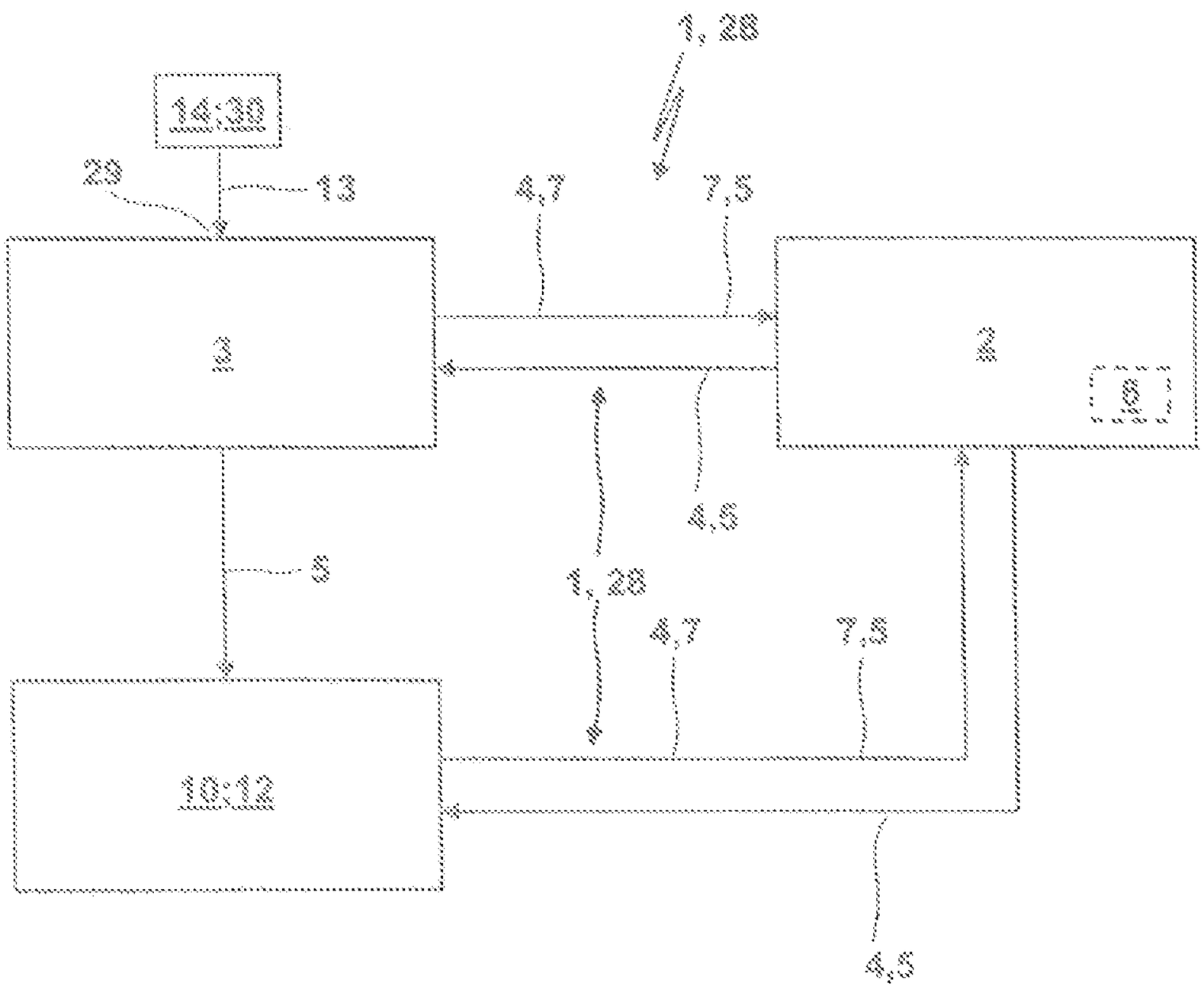

1,28
14;30
29
13
4,7
7,5
3
2
38
4,5
6
1,28
4,7
7,5
10;12
4,5

Fig. 4

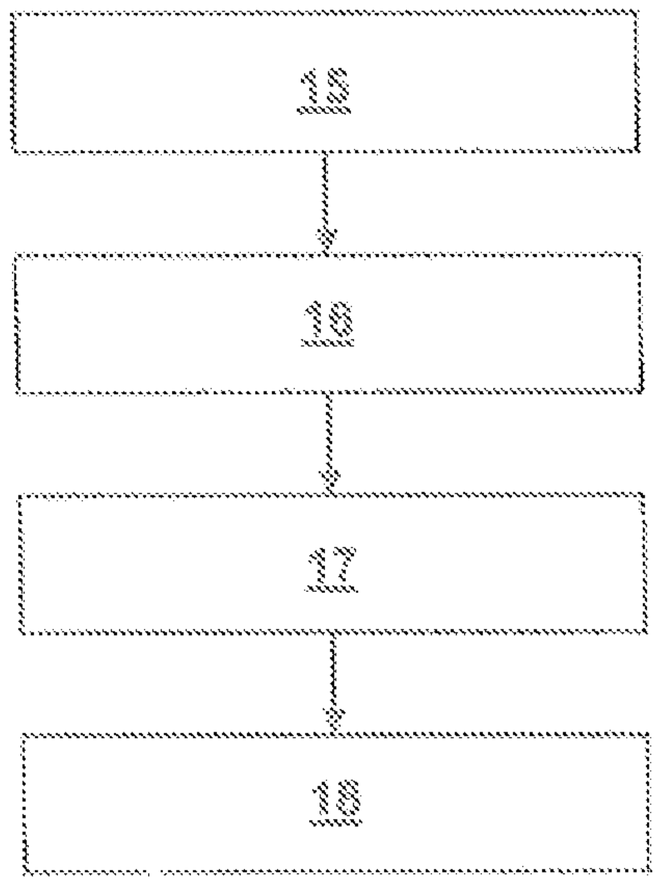


Fig. 5

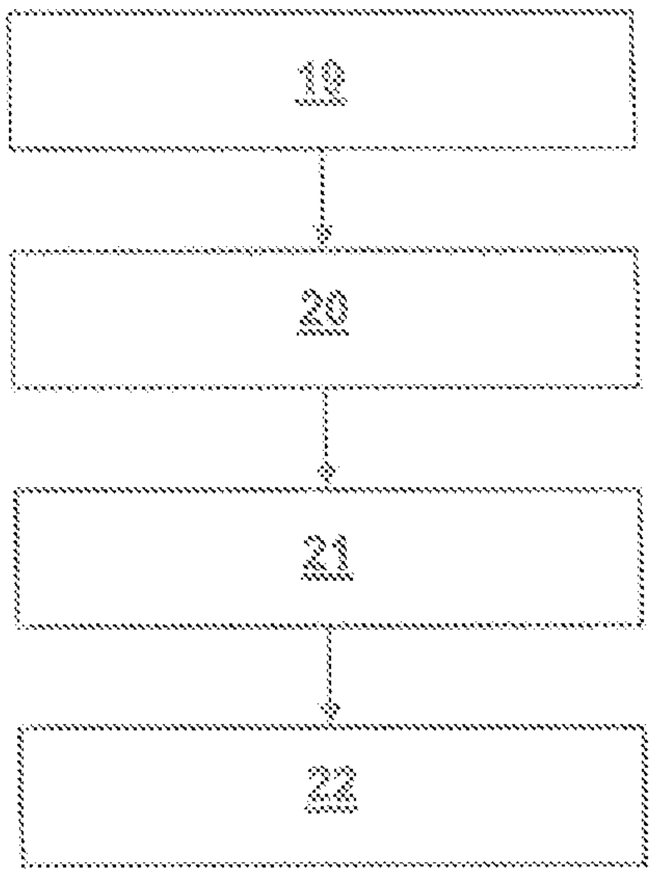


Fig. 6

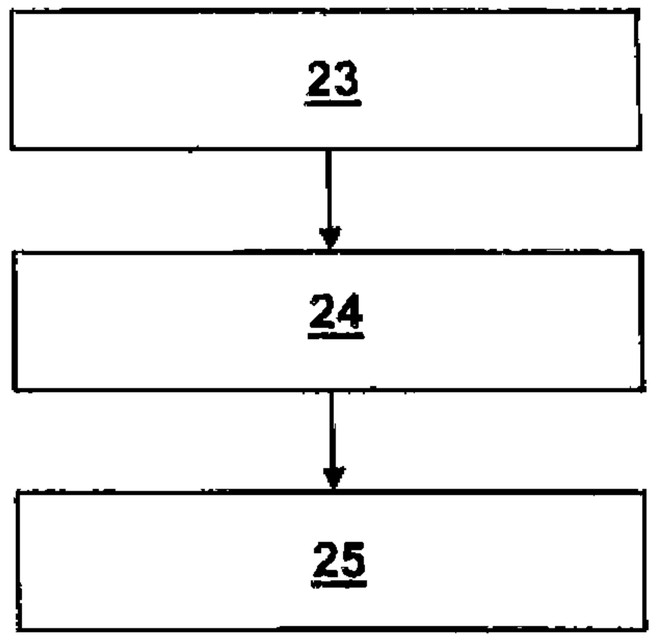


Fig. 7