

SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) CH 712 285 A1

(51) Int. Cl.: G06F 21/60 (2013.01)
G06F 19/00 (2011.01)

Patentanmeldung für die Schweiz und Liechtenstein

Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTANMELDUNG

(21) Anmeldenummer: 00389/16

(71) Anmelder:
Thomas Krech, Thundorferstrasse 194 B
8500 Frauenfeld (CH)

(22) Anmeldedatum: 21.03.2016

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

(43) Anmeldung veröffentlicht: 29.09.2017

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

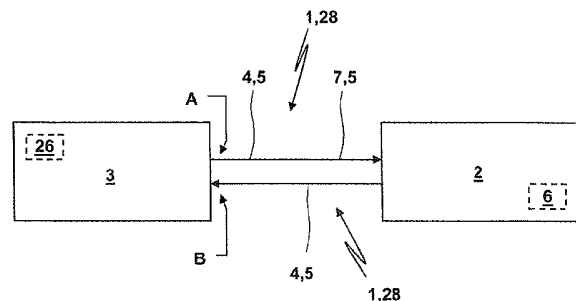
(54) Software mit Steuerlogik zur Umwandlung personalisierter persönlicher Daten in de-personalisierte persönliche Daten und Übermittlung der de-personalisierten Daten an einen Server.

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

Das persönliche 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 Rechneinheit 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 Rechneinheit (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.

[0003] 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.

[0004] 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-you-should-own-your-health-data-loc-pham>).

[0005] 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/>).

[0006] 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-allgemeinArzte-deutschland-potenzial/>) 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 persönlicher 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

[0007] Der Erfindung liegt die Aufgabe zugrunde, ein persönliches Daten-Netzwerk (1, 28) sowie eine Software mit Steuerlogik für den Einsatz in einem persönlichen 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

[0008] 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

[0009] In einem erfindungsgemässen persönlichen 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 so-

nannten Wearables 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.

[0010] Des Weiteren verfügt das erfindungsgemässe persönliche Daten-Netzwerk über eine Rechneinheit, die einem Nutzer zugeordnet ist. Um diesbezüglich einige nicht beschränkende Beispiele zu nennen, kann es sich bei der dem Nutzer zugeordneten Rechneinheit um einen Computer, ein Tablet, ein Mobiltelefon, ein Smartphone, eine Smartwatch, ein Wearable oder einen PDA handeln.

[0011] Im Rahmen der Erfindung kommunizieren die Rechneinheit 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 Rechneinheit zu ermöglichen, und andererseits erfolgen, um eine Übertragung von persönlichen Daten von der Rechneinheit zu der Servereinrichtung zwecks Abspeicherung auf der Servereinrichtung zu ermöglichen.

[0012] 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.

[0013] 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 Rechneinheit, 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 Rechneinheit, 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.

[0014] 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.

[0015] Die Erfindung schlägt vor, dass die Rechneinheit, 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 Rechneinheit übertragen, womit letztendlich dem Nutzer die diesem Nutzer zugeordneten de-personalisierten persönlichen Daten übermittelt werden, womit diese dem Nutzer zur Einsichtnahme bereitgestellt werden können.

[0016] 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 Rechneinheit des Nutzers unter Verwendung der Zuordnungsvorschrift in de-personalisierte persönliche Daten umgewandelt werden. Mit der Steuerlogik der Rechneinheit 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 Rechneinheit, aber nicht auf anderen Teilen des persönlichen Daten-Netzwerks vor. Möglich ist, diese persönlichen Daten nach der Übermittlung auf der Rechneinheit zu löschen.

[0017] Möglich ist, dass ergänzend eine Authentifizierung des Nutzers und/oder der Rechneinheit 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 Rechneinheit 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.

[0018] Ein weiterer Aspekt der Erfindung widmet sich der Problematik, dass nicht lediglich die Kennzeichnung, eine Datei-Bezeichnung, 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 Rechneinheit 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 Teilmعلومات enthalten ist, welche dann aber einen Rückschluss auf den Nutzer nicht mehr oder nur in reduziertem Ausmass ermöglicht.

[0019] Für eine automatische Identifikation der persönlichen Informationen zwecks Entfernung oder Umwandlung derselben gibt es vielfältige Möglichkeiten. Für einen Vorschlag der Erfindung verfügt die Rechneinheit 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.

[0020] Für ein erfindungsgemässes persönliches Daten-Netzwerk besitzt die Rechneinheit 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 werden, 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 Zeitin-

tervalle 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».

[0021] Für einen weiteren erfindungsgemässen Vorschlag beinhaltet die Erkennungslogik eine Text-, Bild- oder Audioerkennungslgik. 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.

[0022] 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 Rechneinheit des Nutzers Informationseinheit-Daten auf einer Ausgabe der Rechneinheit, 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.

[0023] 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 Rechneinheit aus den Informationseinheit-Daten entfernte oder umgewandelte persönliche Informationen und solche, die auf die Person rückschliessen lassen gespeichert werden, was vorzugsweise ebenfalls auf der Rechneinheit 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 Rechneinheit 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.

[0024] Durchaus möglich ist, dass in dem persönlichen Daten-Netzwerk ausschliesslich mehrere jeweils einem Nutzer zugeordnete Rechneinheiten mit der Servereinrichtung kommunizieren. Je grösser die Zahl der Nutzer und der zugeordneten Rechneinheiten ist, desto weniger ist eine Zuordnung der de-personalisierten persönlichen Daten zu den Nutzer und Rechneinheiten 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.

[0025] Möglich ist im Rahmen der Erfindung aber auch, dass in das persönliche Daten-Netzwerk weitere Einrichtungen eingebunden sind:

[0026] Für einen Vorschlag der Erfindung sind in das persönliche Daten-Netzwerk Unterstützer-Rechneinrichtungen, insbesondere Rechneinheiten 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-Rechneinrichtung in das persönliche Daten-Netzwerk eingebunden sein können, sind Apotheken, Versicherungen, Banken oder Forschungseinrichtungen, um nur einige zu nennen.

[0027] Soll eine Unterstützer-Rechneinrichtung 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 Rechneinheit selbst die persönlichen Daten an die Unterstützer-Rechneinrichtung 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-Rechneinrichtung übermittelt, womit dann der Zugriff der Unterstützer-Rechneinrichtung auf die Servereinrichtung mit der Abfrage der de-personalisierten persönlichen Daten, die dem Nutzer, hier dem Patienten des Unterstützers gehören, erfolgen kann.

[0028] Möglich ist auch, dass das persönliche 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.

[0029] Die Erfindung schlägt des Weiteren vor, dass die Unterstützer-Rechnereinrichtung, die Analyse-Rechnereinrichtung, die Servereinrichtung und/oder die dem Nutzer zugeordnete Rechneinheit über Steuerlogik verfügt, welche aus den de-personalisierten persönlichen Daten eines Nutzer Befunde ermittelt.

[0030] 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 Zeitintervall nach der vorangegangenen Impfung) erzeugt und an der Rechneinheit des Nutzers zur Anzeige gebracht wird.

[0031] Die Erfindung schlägt auch vor, dass die Unterstützer-Rechnereinrichtung, die Analyse-Rechnereinrichtung, die Servereinrichtung und/oder die dem Nutzer zugeordnete Rechneinheit 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.

[0032] Ebenfalls möglich ist, dass als Erfassungseinrichtung an der Rechneinheit 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.

[0033] Alternativ oder zusätzlich kann die dem Nutzer zugeordnete Rechneinheit über eine Schnittstelle zu einer Vitaldaten-Erfassungseinrichtung, insbesondere einem Puls-Brustgurt, einem Wearable u.ä. verfügen. Hierbei wird unter einem «Wearable» eine Rechneinheit 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.

[0034] Problematisch kann bei dem persönlichen Daten-Netzwerk sein, dass zwar die persönlichen Daten zwischen der Rechneinheit 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 Rechneinheit 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 Rechneinheit und der Servereinrichtung eine Übertragungspfad-Trenneinrichtung zwischengeschaltet, welche die von der Rechneinheit 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 Rechneinheit 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.

[0035] Eine weitere Ausgestaltung der Erfindung widmet sich der Registrierung des Nutzers. Gemäss einem Vorschlag verfügt die dem Nutzer zugeordnete Rechneinheit über Steuerlogik, die eine Telefonnummer der Rechneinheit, insbesondere des Smartphones, aussendet. Von der für die Registrierung zuständigen Einheit, insbesondere der Servereinrichtung, an welche die Telefonnummer von der Rechneinheit ausgesendet worden ist, empfängt dann die Rechneinheit einen Code, welcher eine Authentifizierung der Rechneinheit ermöglicht. Beispielsweise kann die Rechneinheit bei Ausbildung derselben als Smartphone diesen Code als SMS empfangen. Erfindungsgemäss nimmt erst nach dem Empfang des Codes zur Authentifizierung der Rechneinheit die Rechneinheit 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 Rechneinheit gespeichert werden, wobei diese insbesondere nicht über das Netzwerk übertragen werden.

[0036] 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 Rechneinheit ermittelt wird. Mit der ermittelten neuen Kennzeich-

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

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

[0037] Bei den zuvor genannten Ereignissen, zu denen eine neue Zuordnungsvorschrift mit einer neuen Kennzeichnung von der Steuerlogik der Rechneinheit 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 Rechneinheit und/oder die Unterstützungseinrichtung handeln. Alternativ oder zusätzlich kann als Ereignis verwendet werden, dass eine Übermittlung der Zuordnungsvorschrift an eine Unterstützungseinrichtung erfolgt ist.

[0038] 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.

[0039] Angestrebt sein kann, dass der Nutzer über die Rechneinheit alleinigen personalisierten Zugriff auf seine persönlichen Daten hat. Problematisch kann dies aber u.U. bei Verlust der Rechneinheit, Ohnmacht oder Handlungsunfähigkeit des Nutzers sein. Möglich ist, dass für die Vorsorge für derartige Fälle mittels der Steuerlogik der Rechneinheit die Zuordnungsvorschrift an eine einer Vertrauensperson zugeordnete Rechneinheit übermittelt wird. Bei der Vertrauensperson handelt es sich bspw. um einen Ehepartner, einen für den Nutzer im Notfall zur Entscheidung bevollmächtigte Person oder eine Sicherheitsperson oder eine Person mit Treuhandfunktion, über welche bei Verlust der Rechneinheit ein Zugriff auf die persönlichen Daten möglich bleiben soll. Der der Vertrauensperson zugeordneten Rechneinheit kann dann ein zumindest teilweiser Zugriff auf die de-personalisierten persönlichen Daten und deren Umwandlung in personalisierte persönlichen Daten ermöglicht sein.

[0040] 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.

[0041] Neben dem persönlichen 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.

[0042] Vorteilhafte Weiterbildungen der Erfindung ergeben sich aus den Patentansprüchen, der Beschreibung und den Zeichnungen. 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 Anmeldung unterlagen 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. Die Kombination von Merkmalen unterschiedlicher Ausführungsformen der Erfindung oder von Merkmalen unterschiedlicher Patentansprüche ist ebenfalls abweichend von den gewählten Rückbeziehungen der Patentansprüche möglich und wird hiermit angeregt. Dies betrifft auch solche Merkmale, die in separaten Zeichnungen dargestellt sind oder bei deren Beschreibung genannt werden. Diese Merkmale können auch mit Merkmalen unterschiedlicher Patentansprüche kombiniert werden. Ebenso können in den Patentansprüchen aufgeführte Merkmale für weitere Ausführungsformen der Erfindung entfallen.

[0043] 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.

[0044] 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

[0045] 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 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 persönlichen Daten von einer Servereinrichtung betrifft.

FIGURENBESCHREIBUNG

[0046] Fig. 1 zeigt stark schematisiert ein Daten-Netzwerk 1 mit einer Servereinrichtung 2 und einer einem Nutzer oder Patienten zugeordneten Rechneinheit 3 von einer Vielzahl von mit der Servereinrichtung 2 über ein Netzwerk 1, 28 kommunizierenden, hier nicht dargestellten weiteren Rechneinheiten. Von der Rechneinheit 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 Rechneinheit 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 Rechneinheit 3 zu senden. Die De-personalisierung findet durch eine Software A auf der Rechneinheit 3 statt, die Re-personalisierung durch eine Software B auf der Rechneinheit 3.

[0047] Um zu vermeiden, dass in der Servereinrichtung 2 über eine anfordernde IP-Adresse der Rechneinheit 3 bereits eine Zuordnung der gespeicherten de-personalisierten persönlichen Daten 4 möglich ist, kann zwischen Servereinrichtung 2 und Rechneinheit 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 Rechneinheit 3 und sendet diese mit der eigenen IP-Adresse ohne Hinweis auf die IP-Adresse der Rechneinheit 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 Rechneinheit 3 die de-personalisierten persönlichen Daten 4 überträgt.

[0048] Bei ansonsten Fig. 1 entsprechender Kommunikation zwischen der Rechneinheit 3 und der Servereinrichtung 2 verfügt gemäss Fig. 3 das Daten-Netzwerk 1 über eine Unterstützer-Rechneinrichtung 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 Rechneinheit 3 de-personalisierte persönliche Daten 31 an die Unterstützer-Rechneinrichtung 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 Rechneinheit 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-Rechneinrichtung 10 kann eine Analyse-Rechneinrichtung 11 Zugriff auf die de-personalisierten persönlichen Daten 33 einer Mehrzahl von Nutzern durch Kommunikation mit der Servereinrichtung 2 haben. In der Analyse-Rechneinrichtung 11 kann dann eine Vielzahl von de-personalisierten persönlichen Daten 33 analysiert werden und das Analyseergebnis 32 der Analyse-Rechneinrichtung 11 kann an die Servereinrichtung 2 oder andere Einrichtungen übertragen werden. Möglich ist durchaus auch, dass de-personalisierte persönliche Daten von der Unterstützer-Rechneinrichtung 10 an eine Analyse-Rechneinrichtung 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 Analyseschchnittstelle 27 der Servereinrichtung 2. Das Ergebnis der Analyse kann dann in de-personalisierter Form an die Unterstützer-Rechnereinrichtung 10 oder die Rechneinheit 3 des Nutzers zur weiteren Verarbeitung übertragen werden.

[0049] 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 Rechneinheit 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.

[0050] Als optionale weitere Möglichkeit ist in Fig. 4 dargestellt, dass die Rechneinheit 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 Rechneinheit 3 bildenden Smartphones entstammen können.

[0051] Fig. 5 zeigt beispielhaft ein Verfahren für eine erstmalige Registrierung eines Nutzers durch die diesem zugeordnete Rechneinheit 3:

[0052] Nach dem Laden einer Applikation bspw. auf die als Smartphone ausgebildete Rechneinheit 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 Rechneinheit 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 Rechneinheit 3 nicht als Smartphone, sondern bspw. als Desktop-Version ausgebildet ist, auf welche die Applikation geladen werden kann.

[0053] Optional kann in einem weiteren Verfahrensschritt bei der Rechneinheit 3 angefragt werden, ob eine weitere Rechneinheit 3 als berechtigt hinsichtlich des Nutzers registriert werden soll. Für diesen Fall wird dann die bspw. einem weiteren Smartphone zugeordnete weitere Telefonnummer von der Rechneinheit 3 an die Servereinrichtung 2 übermittelt.

[0054] 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.

[0055] 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.

[0056] Fig. 6 zeigt die Übermittlung von de-personalisierten persönlichen Daten an die Servereinrichtung 2 zwecks Speicherung derselben:

[0057] Die zunächst genannten Verfahrensschritte werden entweder von der Rechneinheit 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.

[0058] 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.

[0059] Fig. 7 zeigt das Verfahren für das Laden von de-personalisierten Daten von der Servereinrichtung 2 in die Rechneinheit 3 (Fig. 1) bzw. in die Unterstützer-Rechnereinrichtung 10 oder Vertrauensperson-Rechnereinheit 12 (vgl. Fig. 4):

[0060] In einem Verfahrensschritt 23 übermittelt die Rechneinheit 3 (bzw. die Unterstützer-Rechneinrichtung 10 oder die Vertrauensperson-Rechneinheit 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 Rechneinheit 3 (bzw. die Unterstützer-Rechneinheit 10 oder die Vertrauensperson-Rechneinheit 12) übertragen, wo sie re-personalisiert werden, indem z.B. in einer Kopfzeile (Header) die Daten zur Person aufgeführt werden.

[0061] 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.

[0062] Eine Applikation der Rechneinheit 3 kann eine Suchfunktion beinhalten, um ein einfaches Wiederauffinden von Informationen zu ermöglichen.

[0063] 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-buzz/5-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-wear-sens-food-diary-you-can-wear-around-your-neck-324508>),
- Google smart pill, um Krebs zu entdecken (vgl. <http://mobihealthnews.com/37730/google-x-developing-cancer-scanning-pill-that-transmits-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/>).

[0064] Eine in das Daten-Netzwerk 1 integrierte Analyseeinrichtung kann eine Vielzahl von depersonalisierten 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](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 wissenschaftlichen Zwecken.

[0065] Auf der Rechneinheit 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.

[0066] 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.

[0067] Eine Applikation einer als Smartphone ausgebildeten Rechneinrichtung 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.

[0068] 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.

[0069] 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 Rechneinheit 3 oder der Servereinrichtung 2 steuern.

[0070] 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 Rechneinheit 3, welche ausschliesslich die Zuordnungsvorschrift beinhaltet, verlorengegangen ist.

[0071] Möglich ist, dass im Rahmen der Erfindung ein auf der Internet-Seite <https://validic.com/api> beschriebenes Verfahren Einsatz findet.

[0072] 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

[0073]

- 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 Rechneinheit (vom Nutzer kontrollierte elektronische Einrichtung, wie z.B. Smartphone, Tablett-PC, Desktop-PC, zur Aufnahme, Verarbeitung, Verwaltung und De-Personalisierung von Daten)
- 4 De-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 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).
- 12 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 (1, 28) mit

- a) einer Servereinrichtung (2), auf welcher persönliche, sensible Daten eines Nutzers gespeichert sind, und
 - b) einer einem Nutzer zugeordneten Rechneinheit (3),
 - c) wobei die Rechneinheit (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 Rechneinheit (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 Rechneinheit (3) über Steuerlogik verfügt, mittels welcher
 - a) eine Anforderung (7) an die Servereinrichtung (2) hinsichtlich der Übermittlung der de-personalisierten persönlichen Daten (4) erzeugt wird, 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 Rechneinheit (3) übermittelten de-personalisierten persönlichen Daten (4), welchen die Kennzeichnung (5) zugeordnet ist, empfangen werden und/oder
 - b) personalisierte persönliche Daten auf der Rechneinheit (3) unter Verwendung der Zuordnungsvorschrift in de-personalisierte persönliche Daten (4) mit zugeordneter Kennzeichnung (5) umwandelt werden und dann die de-personalisierten persönlichen Daten (4) mit der zugeordneten Kennzeichnung (5) von der Rechneinheit (3) über das Netzwerk (1, 28) an die Servereinrichtung (2) übermittelt werden.
2. Daten-Netzwerk (1, 28) nach Anspruch 1, dadurch gekennzeichnet, dass die dem Nutzer zugeordnete Rechneinheit (3) ein Computer, ein Tablet, ein Mobiltelefon, ein Smartphone, eine Smartwatch, ein Wearable oder ein PDA ist.
3. Persönliches Daten-Netzwerk (1, 28) nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die dem Nutzer zugeordnete Rechneinheit (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 und Informationen, die Rückschluss auf die Person zulassen,
- a) automatisch und/oder
 - b) manuell von dem Nutzer
- entfernt oder umgewandelt werden können.
4. Daten-Netzwerk (1, 28) nach Anspruch 3, dadurch gekennzeichnet, dass die dem Nutzer zugeordnete Rechneinheit (3) über eine Steuerlogik verfügt, welche eine Erkennungslogik beinhaltet, mittels welcher automatisch persönliche Informationen und solche, die auf die Person rückschliessen lassen und solche, die auf die Person rückschliessen lassen, in den Informationseinheit-Daten erkannt und aus den Informationseinheit-Daten entfernt werden können.
5. Daten-Netzwerk (1, 28) nach Anspruch 3 oder 4, dadurch gekennzeichnet, dass die dem Nutzer zugeordnete Rechneinheit (3) über eine Steuerlogik verfügt, welche persönliche Informationen und solche, die auf die Person rückschliessen lassen und solche, die auf die Person rückschliessen lassen in verallgemeinerte persönliche Informationen und solche, die auf die Person rückschliessen lassen umwandelt.
6. Persönliches Daten-Netzwerk (1, 28) nach einem der Ansprüche 3 bis 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 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 und solche, die auf die Person rückschliessen lassen, umwandelt.

7. Persönliches Daten-Netzwerk nach einem der Ansprüche 3 bis 6, dadurch gekennzeichnet, dass die dem Nutzer zugeordnete Rechneinheit (3) über Steuerlogik verfügt,
 - a) mittels welcher Informationseinheit-Daten auf einer Ausgabe der Rechneinheit (3) ausgegeben werden, 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 und solche, die auf die Person rückschliessen lassen umzuwandeln.
8. Persönliches Daten-Netzwerk (1, 28) nach einem der Ansprüche 3 bis 7, dadurch gekennzeichnet, dass die dem Nutzer zugeordnete Rechneinheit (3) über Steuerlogik verfügt,
 - a) mittels welcher aus den Informationseinheit-Daten entfernte oder in verallgemeinerte persönliche Informationen und solche, die auf die Person rückschliessen lassen umgewandelte persönliche Informationen und solche, die auf die Person rückschliessen lassen gespeichert werden 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 und solche, die auf die Person rückschliessen lassen umgewandelt worden sind, und
 - bb) den gespeicherten persönlichen Informationen eine zumindest teilweise Rekonstruktion der ursprünglichen Informationseinheit-Daten mit den persönlichen Informationen vornimmt.
9. Persönliches Daten-Netzwerk (1, 28) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die dem Nutzer zugeordnete Rechneinheit (3) über Steuerlogik verfügt, welche
 - a) eine Übermittlung personalisierter persönlicher Daten (31) und/oder
 - b) eine Übermittlung der Zuordnungsvorschrift an eine Unterstützer-Rechneinrichtung (10) ermöglicht.
10. Persönliches Daten-Netzwerk (1, 28) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine Analyse-Schnittstelle (27) des persönlichen Daten-Netzwerkes (1, 28) mit einer Analyse-Rechneinrichtung (11) verbunden ist.
11. Persönliches Daten-Netzwerk (1, 28) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Unterstützer-Rechneinrichtung (12), die Analyse-Rechneinrichtung (11), die Servereinrichtung (2) und/oder die dem Nutzer zugeordnete Rechneinheit (3) über Steuerlogik verfügt, welche aus den de-personalisierte persönliche Daten (4) eines Nutzers Befunde ermittelt und/oder automatische Nachrichten erzeugt.
12. Persönliches Daten-Netzwerk (1, 28) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Unterstützer-Rechneinrichtung (10), die Analyse-Rechneinrichtung (11), die Servereinrichtung (2) und/oder die dem Nutzer zugeordnete Rechneinheit (3) über eine Erfassungseinrichtung (26) verfügt, über welche personalisierte oder de-personalisierte persönliche Daten erfasst werden können.
13. Persönliches Daten-Netzwerk (1, 28) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die dem Nutzer zugeordnete Rechneinheit (3) über eine Schnittstelle (29) zu einer Vitaldaten-Erfassungseinrichtung (30) verfügt.
14. Persönliches Daten-Netzwerk (1, 28) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass zwischen die dem Nutzer zugeordnete Rechneinheit (3) und der Servereinrichtung (2) eine Übertragungspfad-Trenneinrichtung (9) zwischengeschaltet, welche die von der Rechneinheit (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 Rechneinheit (3) unmöglich macht.
15. Persönliches Daten-Netzwerk (1, 28) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass für eine Registrierung des Nutzers die dem Nutzer zugeordnete Rechneinheit (3) über Steuerlogik verfügt, welche
 - a) eine Telefonnummer der Rechneinheit (3) ausgesendet,
 - b) einen Code zur Authentifizierung der Rechneinheit (3) empfängt und
 - c)

erst nach dem Empfang des Codes zur Authentifizierung der Rechneinheit (3) Daten zur Person des Nutzers aufnimmt, welche dann in der Rechneinheit (3) gespeichert werden.

16. Das persönliche Daten-Netzwerk (1, 28) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die dem Nutzer zugeordnete Rechneinheit (3) über Steuerlogik verfügt,
 - a) welche
 - aa) nach dem Übertragen der de-personalisierten persönlichen Daten (4) von der Servereinrichtung (2) an die Rechneinheit (3) und/oder die Unterstützer-Rechneinrichtung (10) und/oder
 - ab) nach einer Übermittlung der Zuordnungsvorschrift oder Kennzeichnung (5) an eine Unterstützer-Rechneinrichtung (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 Rechneinheit (3) über das Netzwerk (1, 28) an die Servereinrichtung (2) übermittelt.
17. Daten-Netzwerk (1, 28) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Zuordnungsvorschrift an eine einer Vertrauensperson zugeordnete Vertrauensperson-Rechneinheit (12) übermittelt wird und der Vertrauensperson-Rechneinheit (12) ein zumindest teilweiser Zugriff auf die de-personalisierten persönlichen Daten und deren Umwandlung in personalisierte persönliche Daten ermöglicht wird.
18. Persönliches Daten-Netzwerk (1, 28) nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die de-personalisierten persönlichen Daten (4) hinsichtlich des Nutzers
 - a) das Geburtsjahr,
 - b) das Geschlecht,
 - c) die ethnische Zugehörigkeit
 - d) die Zugehörigkeit zu einer Rasse und/oder
 - e) das Land des Wohnorts
beinhalten.
19. Software mit Steuerlogik für den Einsatz in einem persönlichen Daten-Netzwerk (1, 28) nach einem der vorhergehenden Ansprüche.

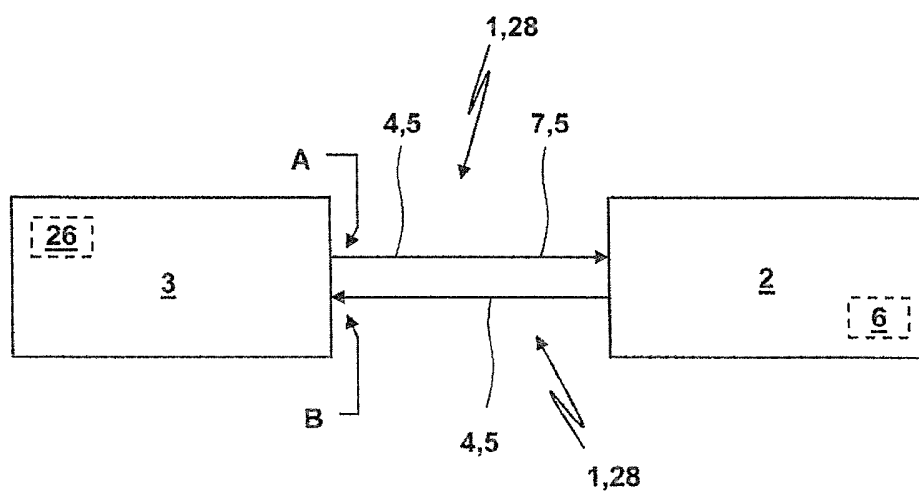


Fig. 1

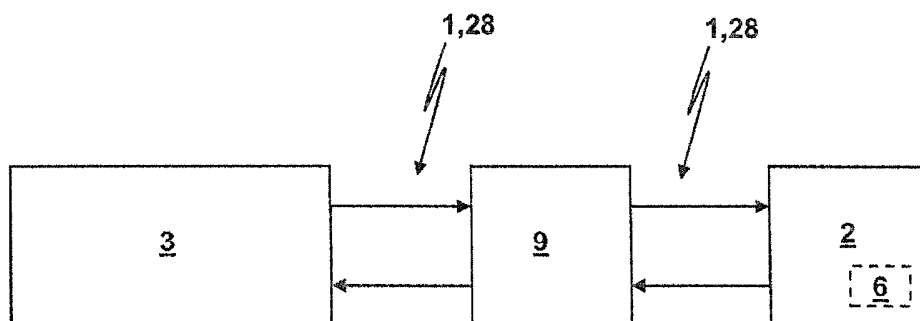


Fig. 2

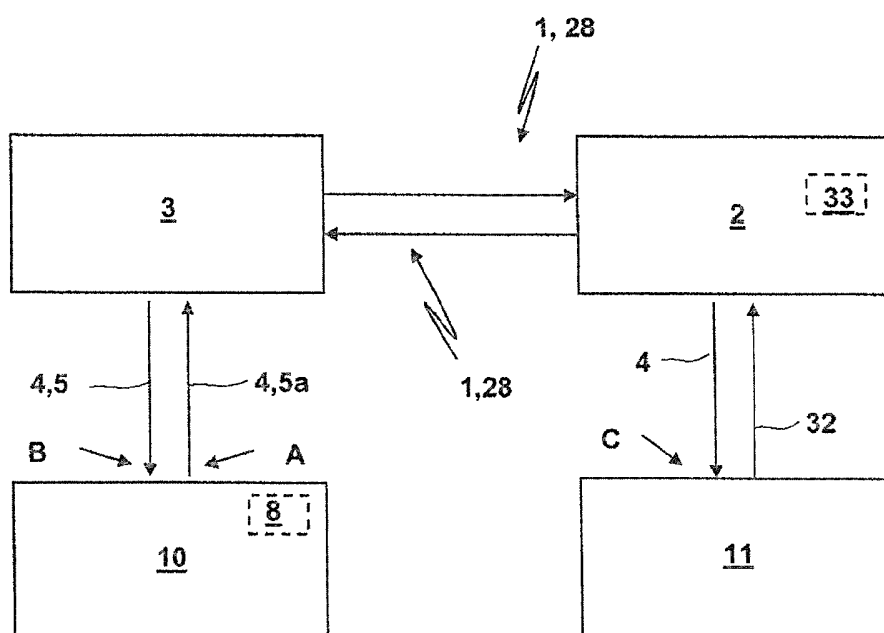


Fig. 3

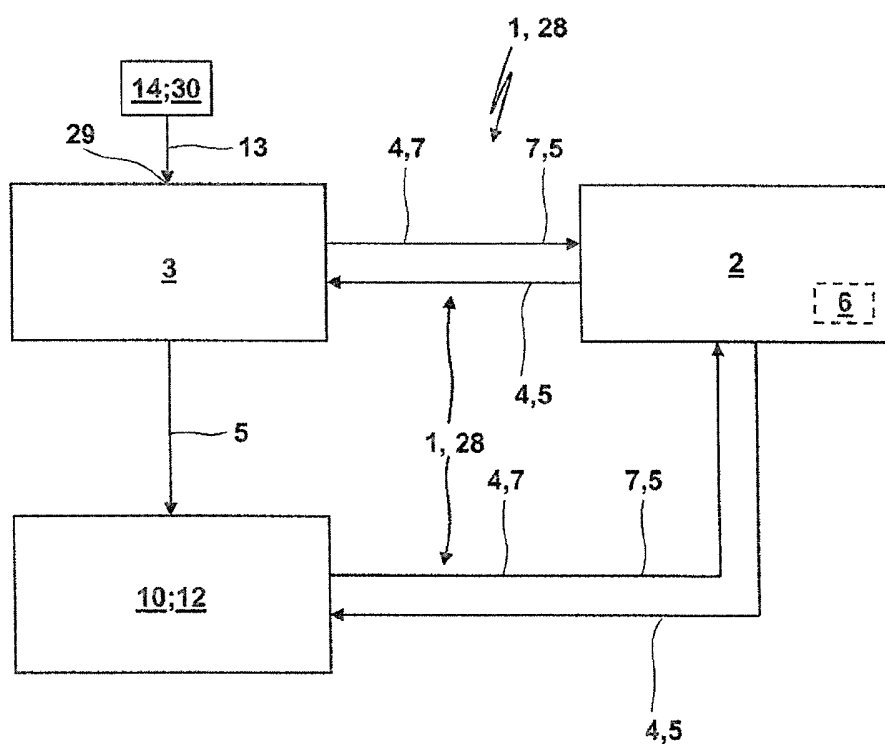


Fig. 4

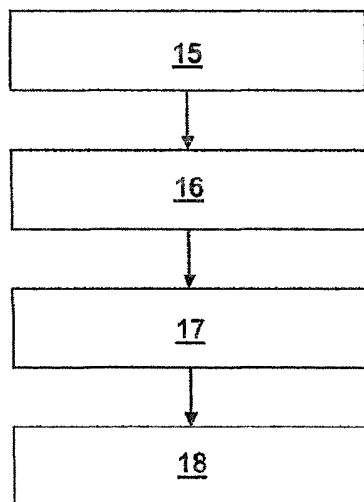


Fig. 5

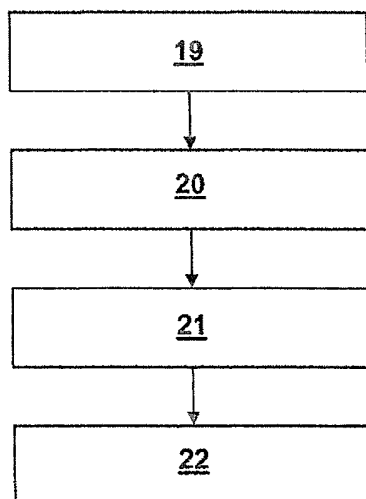


Fig. 6

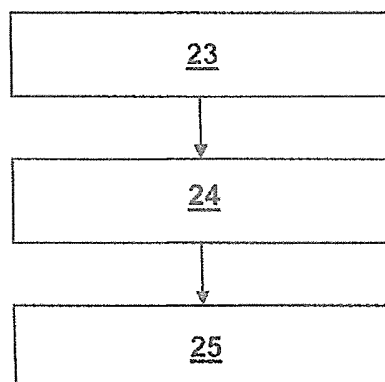


Fig. 7

**VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS**

BERICHT ÜBER DIE RECHERCHE INTERNATIONALER ART

KENNZEICHNUNG DER NATIONALEN ANMELDUNG		AKTENZEICHEN DES ANMELDERS ODER ANWALTS	
		16579-19812	
Nationales Aktenzeichen		Anmeldedatum	
3892016		21-03-2016	
Anmeldeland		Beanspruchtes Prioritätsdatum	
CH			
Anmelder (Name)			
rothomed.ch GmbH			
Datum des Antrags auf eine Recherche internationaler Art		Nummer, die die internationale Recherchenbehörde dem Antrag auf eine Recherche internationaler Art zugestellt hat	
26-09-2016		SN67432	
I. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDS (treffen mehrere Klassifikationssymbole zu, so sind alle anzugeben)			
Nach der internationalen Patentklassifikation (IPC) oder sowohl nach der nationalen Klassifikation als auch nach der IPC			
G06F19/00			
II. RECHERCHIERTE SACHGEBIETE			
Recherchierter Mindestprüfstoff			
Klassifikationssystem	Klassifikationssymbole		
IPC	G06F		
Recherchierte, nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Sachgebiete fallen			
III. ☐ EINIGE ANSPRÜCHE HABEN SICH ALS NICHT RECHERCHIERBAR ERWIESEN (Bemerkungen auf Ergänzungsbogen)			
IV. ☐ MANGELNDE EINHEITLICHKEIT DER ERFINDUNG (Bemerkungen auf Ergänzungsbogen)			

Formblatt PCT/ISA 201 a (11/2000)

BERICHT ÜBER DIE RECHERCHE INTERNATIONALER ART

Nr. des Antrags auf Recherche

CH 3892016

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES INV. G06F19/00 ADD.		
Nach der internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPK		
B. RECHERCHIERTE BEREICHE Recherchierte Mindestprüfstoff (Klassifikationsystem und Klassifikationsymbole) G06F		
Rechenhilfe, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen		
Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe) EPO-Internal, INSPEC, WPI Data		
C. ALS WESENTLICH ANGESEHENE VERÖFFENTLICHUNGEN		
Kategorie	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Beiz. Anspruch Nr.
X	WO 01/18631 A1 (MEDICAL DATA SERVICES GMBH [DE]; ELFERING INGO [US]) 15. März 2001 (2001-03-15) * Seite 1, Zeile 2 - Zeile 21 * * Seite 2, Zeile 28 - Seite 3, Zeile 23 * * Seite 9, Zeile 27 - Seite 11, Zeile 26 * -----	1-19
X	EP 1 939 785 A2 (SURVEILLANCE DATA INC [US]) 2. Juli 2008 (2008-07-02) * Zusammenfassung * * Absatz [0002] * * Absatz [0005] - Absatz [0006] * * Absatz [0009] * * Absatz [0024] - Absatz [0026] * * Absatz [0031] - Absatz [0036] * * Absatz [0040] - Absatz [0044] * * Abbildungen 1-3 * ----- -/-	1-19
☒	Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen	☒ Siehe Anhang Patentanhänge
* Besondere Kategorien von angegebenen Veröffentlichungen : "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist "B" Dieses Dokument, das jedoch auf ein oder nach dem Anmeldedatum veröffentlicht worden ist "C" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelsfrei erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchierten Bereich veröffentlichten Veröffentlichung belegt werden soll, oder die aus einem anderen besonderen Grund angegeben ist (wie angegeben) "D" Veröffentlichung, die sich auf eine technische Offenbarung, eine Benutzung, eine Ausgestaltung oder andere Maßnahmen bezieht "E" Veröffentlichung, die vor dem Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist "F" Spätere Veröffentlichung, die nach dem Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis der Erfindung zugrundeliegenden Prinzipien oder der ihr zugrundeliegenden Theorie angegeben ist "G" Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden "H" Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist "I" Veröffentlichung, die Mitglied derselben Patentfamilie ist		
Datum des tatsächlichen Abschlusses der Recherche internationaler Art 14. Dezember 2016		Abschließdatum des Berichts über die Recherche internationaler Art 02 JAN 2017
Name und Postanschrift der internationalen Recherchehörde Europäisches Patentamt, P. B. 5518 Patentamt 2 NL - 2260 HV Rijswijk Tel. (+31-70) 340-2040 Fax (+31-70) 340-3018		Berechtigter Beauftragter Konak, Eyüp

Formblatt PCT/ISA/205 (Blatt 2) (Januar 2004)

Seite 1 von 2

BERICHT ÜBER DIE RECHERCHE INTERNATIONALER ART

Nr. des Antrags auf Recherche

CH 3892016

C (Fortsetzung): ALS WESENTLICH ANGESEHENE VERÖFFENTLICHUNGEN		
Kategorie	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2006/179073 A1 (KIMURA SHINYA [JP]) 19. August 2006 (2006-08-18) * Abbildung 5 * * Absatz [0069] - Absatz [0078] * *****	1-19
A	US 2015/127382 A1 (AL-SHAYKH OSAMA [US] ET AL) 7. Mai 2015 (2015-05-07) * Zusammenfassung * * Abbildungen 1-3 * * Absatz [0045] - Absatz [0047] * *****	1-19

Formblatt PCT/ISA/205 (Fortsetzung von Blatt 2) (Januar 2009)

Seite 2 von 2

BERICHT ÜBER DIE RECHERCHE INTERNATIONALER ART

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Nr. des Antrags auf Recherche

CH 3892016

Im Fischereibericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 0118631	A1	15-03-2001	KEINE
EP 1939785	A2	02-07-2008	CA 2615292 A1 18-06-2008 EP 1939785 A2 02-07-2008 EP 2953053 A1 09-12-2015 HK 1120316 A1 07-08-2015 US 2008147554 A1 19-06-2008
US 2006179073	A1	10-08-2006	AU 2003227190 A1 11-10-2004 CN 1759403 A 12-04-2006 US 2006179073 A1 10-08-2006 WO 2004084483 A1 30-09-2004
US 2015127382	A1	07-05-2015	KEINE

Formular PG/178A/201 (Führung Patentfamilie) (Juni 2004)