



SLOVENSKI STANDARD
oSIST prEN ISO 25237:2026

01-november-2026

Zdravstvena informatika - Psevdonimizacija (ISO/DIS 25237:2026)

Health informatics - Pseudonymization (ISO/DIS 25237:2026)

Medizinische Informatik - Pseudonymisierung (ISO/DIS 25237:2026)

Informatique de santé - Pseudonymisation (ISO/DIS 25237:2026)

Ta slovenski standard je istoveten z: prEN ISO 25237

ICS:

35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology
-----------	---	--

oSIST prEN ISO 25237:2026

de

Sample Document

get full document from standards.iteh.ai

EUROPÄISCHE NORM
EUROPEAN STANDARD
NORME EUROPÉENNE

ENTWURF
prEN ISO 25237

Mai 2026

ICS 35.240.80

Vorgesehen als Ersatz für EN ISO 25237:2017

Deutsche Fassung

Medizinische Informatik - Pseudonymisierung (ISO/DIS
25237:2026)

Health informatics - Pseudonymization (ISO/DIS
25237:2026)

Informatique de santé - Pseudonymisation (ISO/DIS
25237:2026)

Dieser Europäische Norm-Entwurf wird den CEN-Mitgliedern zur parallelen Umfrage vorgelegt. Er wurde vom Technischen Komitee CEN/TC 251 erstellt.

Wenn aus diesem Norm-Entwurf eine Europäische Norm wird, sind die CEN-Mitglieder gehalten, die CEN-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist.

Dieser Europäische Norm-Entwurf wurde von CEN in drei offiziellen Fassungen (Deutsch, Englisch, Französisch) erstellt. Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem CEN-CENELEC-Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Warnvermerk: Dieses Schriftstück hat noch nicht den Status einer Europäischen Norm. Es wird zur Prüfung und Stellungnahme vorgelegt. Es kann sich noch ohne Ankündigung ändern und darf nicht als Europäischen Norm in Bezug genommen werden.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

© 2026 CEN Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den nationalen Mitgliedern von CEN vorbehalten.

Ref. Nr. prEN ISO 25237:2026 D

Inhalt

	Seite
Europäisches Vorwort	5
Vorwort	6
Einleitung	7
1 Anwendungsbereich	9
2 Normative Verweisungen	9
3 Begriffe	10
4 Abkürzung	16
5 Prinzipien der Pseudonymisierung	17
5.1 Allgemeines	17
5.2 Trennung der Bezeichner	17
5.3 Daten-Minimierung	17
6 Anforderungen an die Pseudonymisierung im Gesundheitswesen	18
6.1 Pseudonymisierung	18
6.2 Anonymisierung	19
6.3 Direkte und indirekte Bezeichner	19
6.4 Klassifizierung von Dateninhabern	20
6.4.1 Allgemeines	20
6.4.2 behandelte Person	20
6.4.3 Ärztliches Personal und Organisationen	20
6.4.4 Gerätedaten	21
6.5 Vertrauenswürdiger Dienst	21
6.6 Daten von Opfern von Gewalttaten und öffentlich bekannten Personen	21
6.7 Geninformationen	21
7 Pseudonymisierung in der Praxis	21
7.1 Allgemeines	21
7.2 Datensicherheitsstufe 1: Eliminierung von eindeutig zur Identifizierung geeigneten Daten oder von leicht erhältlichen zur indirekten Identifizierung geeigneten Daten	22
7.3 Datensicherheitsstufe 2: Berücksichtigung von Angreifern, die externe Daten nutzen	22
7.4 Datensicherheitsstufe 3: Berücksichtigung von Datenausreißern	23
8 Praktische Anwendung der Pseudonymisierung und der kontrollierten Wiedererkennung von pseudonymisierten Daten	23
8.1 Allgemeines	23
8.2 Pseudonymisierungsansatz	24
8.3 Wiedererkennung-Zweckcodes	24
9 Eigenschaften von Pseudonymisierungsdiensten	24
9.1 Allgemeines	24
9.2 Mindestanforderungen an vertrauenswürdige Praktiken	25
10 Schutz der Privatsphäre durch Pseudonymisierung	25
10.1 Allgemeines	25
10.2 Eignung von personenbezogenen Informationen zur direkten und zur indirekten Identifizierung	26
10.2.1 Allgemeines	26

10.2.2	Zur Identifizierung von Personen geeignete Variablen.....	26
10.2.3	Kumulationsvariablen.....	27
10.2.4	Ausreißervariablen.....	28
10.2.5	Strukturierte Datenvariablen.....	28
10.2.6	Nicht-strukturierte Datenvariablen.....	29
11	Wiedererkennungsprozess.....	30
11.1	Kontext.....	30
11.1.1	Allgemeines.....	30
11.1.2	Wiedererkennung als Teil der normalen Verfahren.....	30
11.1.3	Wiedererkennung als außergewöhnliches Ereignis.....	31
11.2	Technische Realisierbarkeit.....	32
12	Pseudonymisierungstechniken.....	32
12.1	Allgemeines.....	32
12.2	Schlüsseltechniken.....	32
12.2.1	Tokenisierung.....	32
12.2.2	Verschlüsselungsbasierte Pseudonymisierung.....	33
12.2.3	Hashing.....	33
12.2.4	Deterministische Pseudonymisierung.....	33
12.2.5	Nicht-deterministische oder zufällige Pseudonymisierung.....	33
12.2.6	Datenmaskierung.....	33
Anhang A (informativ)	Pseudonymisierungsszenarien im Gesundheitswesen.....	34
A.1	Allgemeines.....	34
A.2	Erläuterung der Szenarien.....	34
A.3	Szenarien im Gesundheitswesen.....	35
A.3.1	Reihenfolge nach der klinischen Pathologie (pseudonymisierte Pflege).....	39
A.3.2	Klinische Studie.....	40
A.3.3	Klinische Forschung.....	43
A.3.4	Überwachung der öffentlichen Gesundheit.....	45
A.3.5	Berichte zur Patientensicherheit (unerwünschte Ereignisse im Zusammenhang mit Arzneimitteln).....	47
A.3.6	Nicht das Gesundheitswesen betreffende Forschung, die personenbezogene mediale Daten verwendet.....	48
A.3.7	Marktforschung.....	48
A.3.8	Lehrdateien.....	49
A.3.9	Außendienst.....	50
Anhang B (informativ)	Spezifikation von Verfahren und Implementierung.....	55
Anhang C (informativ)	Genetische Informationen.....	57
Anhang D (informativ)	Beispielhafte Kategorien personenbezogener Daten für die Risikobewertung der Re-Identifizierung bei Pseudonymisierung.....	59
Literaturhinweise.....		61

Bilder

Bild A.1 — Veränderung der Daten zu klinischen Studien.....	41
Bild A.2 — Informationsflüsse bei klinischen Studien.....	43
Bild A.3 — Informationsflüsse bezüglich der Patientensicherheit.....	48
Bild A.4 — Datenflüsse.....	50

prEN ISO 25237:2026 (D)

Bild A.5 — Datenvorbereitung.....	52
Bild A.6 — Pseudonymisierungsprozess	53

Tabellen

Tabelle A.1 — Eigenschaften der Szenarien	37
Tabelle A.2.....	50
Tabelle D.1	59

Sample Document

get full document from standards.iteh.ai

Europäisches Vorwort

Dieses Dokument (prEN ISO 25237:2026) wurde vom Technischen Komitee ISO/TC 215 „Health informatics“ in Zusammenarbeit mit dem Technischen Komitee CEN/TC 251 „Medizinische Informatik“ erarbeitet, dessen Sekretariat von NEN gehalten wird.

Dieses Dokument ist derzeit zur parallelen Umfrage vorgelegt.

Dieses Dokument wird EN ISO 25237:2017 ersetzen

Anerkennungsnotiz

Der Text von ISO/DIS 25237:2026 wurde von CEN als prEN ISO 25237:2026 ohne irgendeine Abänderung genehmigt.

Sample Document

get full document from standards.iteh.ai

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsinstitute (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Normungsthemen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC Directives, Teil 1, beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC Directives, Teil 2, erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Eine Erläuterung der Bedeutung ISO-spezifischer Benennungen und Ausdrücke, die sich auf Konformitätsbewertung beziehen, sowie Informationen über die Beachtung der Grundsätze der Welthandelsorganisation (WTO) zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 215, *Health informatics*, erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (EN ISO 25237:2017), die technisch überarbeitet wurde.

Die wesentlichen Änderungen sind folgende:

- Anpassung an aktualisierte Datenschutz- und Sicherheitsstandards;
- aktualisierte Terminologie, Definitionen und Abkürzungen;
- erweiterte Anleitung zu Pseudonymisierungstechniken und deren Umsetzung;
- verstärkte Hinweise zu Governance, Interoperabilität und Risikomanagement;
- Aufnahme aktualisierter Implementierungsleitlinien und Anwendungsfälle.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html zu finden.

Einleitung

Die Pseudonymisierung stellt ein wichtiges Mittel zum Schutz der Privatsphäre von personenbezogenen Gesundheitsinformationen in der sich entwickelnden digitalen Landschaft dar. Mit der wachsenden Komplexität der Gesundheitssysteme und dem steigenden Bedarf an Daten (3.10), die über verschiedene Plattformen, Organisationen und Rechtsgebiete für eine Reihe von verschiedenen Zwecken geteilt werden müssen, hilft die Pseudonymisierung, die Nachfrage nach Datennutzung mit dem Bedarf an starken Datenschutzmaßnahmen in Einklang zu bringen.

Dieses Dokument ist darauf ausgelegt, Organisationen bei der Implementierung von Pseudonymisierungsprozessen zu unterstützen, um ein hohes Maß an Datenschutz zu ermöglichen und gleichzeitig die Nutzbarkeit von Daten im Gesundheitswesen zu ermöglichen. Die Spezifikation eines allgemeinen Ablaufplans dient in Verbindung mit einer Politik bzw. Policy für vertrauenswürdige Vorgänge sowohl als allgemeiner Leitfaden für Implementierer als auch zu Qualitätssicherungszwecken, indem sie den Anwendern der Pseudonymisierungsdienste dabei hilft, zu ermitteln, inwieweit sie diesen Diensten vertrauen können. Die in diesem Dokument dargelegten Konzepte und Prozesse dienen dazu, Organisationen in die Lage zu versetzen, die Pseudonymisierung selbst in einer Weise auszuführen, um den gewünschten Gütegrad und die gewünschte Risikominderung zu erreichen.

Anwendbare Bereiche für die Pseudonymisierung umfassen:

- die indirekte Nutzung von klinischen Daten (z. B. zu Forschungszwecken);
- klinische Studien und die Überwachung nach Markteinführung;
- pseudonymisierte Pflege;
- Überwachung und Bewertung der öffentlichen Gesundheit;
- Berichte zur Patientensicherheit;
- vergleichende und nicht-vergleichende Berichte zu Qualitätsindikatoren;
- Kreuzgutachten (Peer-Reviews);
- Verbrauchergesundheitsdienste;
- Patientenerkennungssysteme;
- vertrauliche Berichte zur Patientensicherheit (z. B. zu Nebenwirkungen von Medikamenten).

Dieses Dokument wurde aktualisiert, um Änderungen seit der vorherigen Ausgabe von 2017 unter Berücksichtigung folgender Aspekte widerzuspiegeln:

- ein sich ständig weiterentwickelndes regulatorisches Umfeld mit der Einführung neuer oder überarbeiteter Datenschutzgesetze wie der DSGVO, HIPAA, dem EU- Datenschutzgesetz und anderen;
- neue und/oder überarbeitete Standards und Leitlinien, und
- die sich wandelnde technologische Landschaft, insbesondere die beschleunigte Einführung künstlicher Intelligenz.

Dieses Dokument betont die Bedeutung der Pseudonymisierung für den Schutz von Patientendaten und der Privatsphäre von Patienten im Kontext dieser neuen Vorschriften und Technologien. Pseudonymisierung bietet nicht nur Schutz der Privatsphäre, sondern spielt auch eine entscheidende Rolle bei der Ermöglichung

prEN ISO 25237:2026 (D)

von Forschung, Innovation und Verbesserung von Gesundheitsdienstleistungen und fördert gleichzeitig das Vertrauen in die Praktiken der Datenverarbeitung.

Sample Document

get full document from standards.iteh.ai

1 Anwendungsbereich

Dieses Dokument legt Grundsätze für den Schutz der Privatsphäre durch Pseudonymisierungsdienste fest, die darauf abzielen, personenbezogene Gesundheitsinformationen zu schützen. Es gilt für Organisationen, die Pseudonymisierungsprozesse implementieren oder Vertrauenswürdigkeit in Pseudonymisierungsservice-Vorgängen beanspruchen. Dieses Dokument:

- legt grundlegende Prinzipien für die Pseudonymisierung fest;
- passt sich aktualisierten Vorschriften und Standards wie ISO/IEC 20889:2018, ISO/IEC 27559:2022 und anderen relevanten Dokumenten sowie Methodologien für Pseudonymisierungsdienste an;
- bietet Anleitungen zur praktischen Anwendung der Pseudonymisierung, einschließlich Beispielen für den De-Identifizierungsprozess, bewährten Verfahren und Fallstudien;
- legt wichtige Elemente im Konzept der Pseudonymisierung, der direkten und indirekten Identifizierbarkeit personenbezogener Daten und verschiedener Arten von Datenvariablen fest;
- bietet Anleitungen zur Risikobewertung für die Wiedererkennung und zwei unterschiedliche Kontexte der Wiedererkennung von pseudonymisierten Informationen; und
- legt verschiedene Techniken fest, die darauf abzielen, den Schutz der Privatsphäre mit der Datenverwendung in Einklang zu bringen, um sicherzustellen, dass die Daten für Analysen, Forschung oder betriebliche Anforderungen genutzt werden können, ohne dass persönliche Identitäten preisgegeben werden.

Darüber hinaus befasst sich dieses Dokument mit neuen regulatorischen und ethischen Rahmenbedingungen, wie dem EU AI Act [1], IEEE 7000:2021 [2], und IEEE 7007:2021 [3], sowie mit Leitlinien zur Pseudonymisierung in der KI unter Berücksichtigung des Einflusses aufkommender Technologien auf den Schutz der Privatsphäre.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 18014-1:2008, *Information technology — Security techniques — Time-stamping services — Part 1: Framework*

ISO/IEC 19794-1:2006, *Information technology — Biometric data interchange formats — Part 1: Framework*

ISO/IEC 20889:2018, *Privacy enhancing data de-identification terminology and classification of techniques*

ISO/TS 22220:2011, *Health informatics — Identification of subjects of health care*

ISO/IEC 27559:2022, *Information security, cybersecurity and privacy protection — Privacy enhancing data de-identification framework*

EN ISO 12052:2017, *Medizinische Informatik — Digitale Bildverarbeitung und Kommunikation in der Medizin (DICOM) inklusive Workflow und Datenmanagement (ISO 12052:2017)*

EN ISO 25237:2017, *Medizinische Informatik — Pseudonymisierung (ISO 25237:2017)*

prEN ISO 25237:2026 (D)

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden *Begriffe*.

ISO und IEC unterhalten terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen:

- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

3.1
Zugriffskontrolle
 Mittel zur Sicherstellung, dass auf die Ressourcen eines *Datenverarbeitungssystems* (3.10) nur von dazu berechtigten Entitäten und in autorisierter Art und Weise zugegriffen werden kann

[QUELLE: ISO/IEC 2382:2015 [4], 2126294]

3.2
Anonymisierung
 Prozess, bei dem *Daten* (3.10), die sich auf einen *Dateninhaber* (3.12) beziehen, entweder vom für die Verarbeitung der *Daten* (3.10) *Verantwortlichen* (3.8) allein oder in Zusammenarbeit mit anderen unumkehrbar so verändert werden, dass sich der *Dateninhaber* (3.12) danach weder direkt noch indirekt identifizieren lässt

Anmerkung 1 zum Begriff: Der Begriff ist absolut und kann in der Praxis schwierig umgesetzt werden.

Anmerkung 2 zum Begriff: Definition aus ISO/IEC 29100:2024 [5] modifiziert durch Ersetzung von Verweisen auf „*persönlich identifizierbare Informationen (PII)*“ und „*PII-Daten*“ durch äquivalente Begriffe, die in dieser Norm verwendet werden.

[QUELLE: ISO/IEC 29100:2024 [5], 3.2, modifiziert]

3.3
anonymisierte Daten
Daten (3.10), die als Ergebnis eines *Anonymisierungsprozesses* (3.2) erzeugt wurden

Anmerkung 1 zum Begriff: Definition aus ISO/IEC 29100:2024 [5] modifiziert durch Ersetzung von „*PII-Anonymisierungsprozess* (3.2)“ durch den in dieser Norm verwendeten äquivalenten Begriff.

[QUELLE: ISO/IEC 29100:2024 [5], 3.3, modifiziert]

3.4
Angreifer
 Person, die bewusst Schwachstellen in technischen und nicht-technischen Sicherheitskontrollen nutzt, um *Informationssysteme* (3.25) und Netzwerke zu stehlen oder zu beeinträchtigen oder die Verfügbarkeit für berechtigte Benutzer des *Informationssystems* (3.25) und Netzwerk-Ressourcen zu beeinträchtigen

[QUELLE: ISO/IEC 27033-1:2015 [6], 3.3]

3.5
Attribut
 inhärente Eigenschaft

[QUELLE: ISO/IEC 20889:2018 [7], 3.2]

3.6

Authentisierung

Bereitstellung von Zusicherung, dass ein behauptetes Merkmal einer Entität korrekt ist

[QUELLE: ISO/IEC 27000:2018 [8], 3.5]

3.7

Vertraulichkeit

Eigenschaft, dass *Informationen* (3.25) keinen unberechtigten Personen, Entitäten oder Prozessen zur Verfügung gestellt oder diesen offenbart werden

[QUELLE: ISO/IEC 27000:2018 [8], 3.10]

3.8

für die Verarbeitung Verantwortlicher

natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der *Verarbeitung von personenbezogenen Daten* (3.32) entscheidet

[QUELLE: ISO/TS 27790:2009 [9], 3.16]

3.9

kryptographischer Algorithmus

<Chiffrierung> Verfahren für die Umwandlung von *Daten* (3.10) mit dem Ziel, deren *Informationsgehalt* (3.25) zu verbergen und ihre unerkannte Änderung und/oder nicht autorisierte Nutzung zu verhindern

[QUELLE: ISO 7498-2:1989 [10], modifiziert]

3.10

Daten

wieder herleitbare Darstellung von *Informationen* (3.25) in einer formalisierten Art und Weise, die zur Kommunikation, Interpretation oder Verarbeitung geeignet ist

Anmerkung 1 zum Begriff: *Daten* (3.10) können durch Menschen oder automatische Mittel verarbeitet werden.

[QUELLE: ISO/IEC 2382:2015 [4], 2121272, modifiziert - Anmerkung 2 und Anmerkung 3 zum Begriff wurden gelöscht.]

3.11

Datenintegrität

Eigenschaft, dass *Daten* (3.10) nicht in unautorisierter Art und Weise verändert oder zerstört worden sind

[QUELLE: ISO 7498-2:1989 [10], 3.3.21]

3.12

Dateninhaber

Entität, auf die sich die *Daten* (3.10) beziehen

Anmerkung 1 zum Begriff: Der Begriff „*Dateninhaber* (3.12)“ ist breiter als „PII-Inhaber“ oder „*Daten*(3.10) -Subjekt“, wie er in Richtlinien und Standards im Zusammenhang mit der *Privatsphäre* (3.31) üblich ist, und kann sich auf eine Entität wie eine Organisation, ein Gerät oder eine Softwareanwendung sowie auf eine *natürliche Person* (3.27) beziehen.

[QUELLE: ISO/IEC 20889:2018 [7], 3.4, modifiziert]

prEN ISO 25237:2026 (D)

3.13

Datenschutz

technisches und soziales System für die Aushandlung, Verwaltung und Sicherstellung der *Vertraulichkeit* (3.31) und Sicherheit von *Informationen* (3.25)

[QUELLE: ISO/TS 14265:2011 [11], 2.9]

3.14

Datensatz

Daten(3.10)erfassung

[QUELLE: ISO/IEC 20889:2018 [7], 3.5]

3.15

Entschlüsselung

Prozess der Konvertierung von verschlüsselten *Daten* (3.10) zurück in die ursprüngliche verständliche Form

3.16

Entpersonalisierungsprozess

Prozess der Aufhebung der Assoziation zwischen einem Satz von *identifizierenden Attributen* (3.33) und dem *Dateninhaber* (3.12)

[QUELLE: ISO/IEC 20889:2018 [7], 3.6]

3.17

direkter Bezeichner

Attribut (3.5), das allein eine eindeutige *Identifizierung* (3.20) eines *Dateninhabers* (3.12) in einem bestimmten Kontext ermöglicht

Anmerkung 1 zum Begriff: Hier und im gesamten Dokument wird der spezifische Kontext berücksichtigt, der die *Informationen* (3.25) enthält, dass die Entität, die die *Daten* (3.10) verarbeitet (z. B. de-identifiziert), zusammen mit *Informationen* (3.25) besitzt, die Dritte und potenzielle Angreifer besitzen können oder die im öffentlichen Bereich sind.

[QUELLE: ISO/IEC 20889:2018 [7], 3.10, modifiziert]

3.18

Offenlegung

Preisgabe von oder Ermöglichung des Zugriffs auf *Daten* (3.10)

Anmerkung 1 zum Begriff: Ob der *Empfänger* (3.37) sich die *Daten* (3.10) tatsächlich ansieht, sie zur Kenntnis nimmt oder sie aufbewahrt, ist ohne Bedeutung für die Frage, ob sie *offengelegt* (3.18) wurden.

3.19

Verschlüsselung

Prozess der Konvertierung von *Informationen* (3.25) oder *Daten* (3.10) in eine Chiffre oder einen Code

3.20

Identifizierung

Prozess der Zuordnung eines Satzes von *identifizierenden Attributen* (3.22) zu einem *Dateninhaber* (3.12)

Anmerkung 1 zum Begriff: Die *Identifikation* (3.20) ermöglicht es, die *Attribute* (3.5), die mit einem *Dateninhaber* (3.12) verbunden sind, von Attributen zu unterscheiden, die mit anderen *Dateninhabern* (3.10) in einem Kontext verbunden sind, wobei der Kontext einen *Datensatz* (3.14) umfassen kann, der durch einen *Entpersonalisierungsprozess* (3.16) erzeugt wird.

Anmerkung 2 zum Begriff: Die *Identifizierung* (3.20) kann sich auf einen *Dateninhaber* (3.12) beziehen, der nicht eine *natürliche Person* (3.27) ist.

3.21

Bezeichner

Satz von *Attributen* (3.5) in einem *Datensatz* (3.14) der es ermöglicht, einen *Dateninhaber* (3.12) innerhalb eines spezifischen Kontextes eindeutig zu *identifizieren* (3.20)

[QUELLE: ISO/IEC 20889:2018 [7], 3, modifiziert]

3.22

Identifizierendes Attribut

Attribut (3.5) in einem *Datensatz* (3.14), das zur eindeutigen Identifizierung eines *Dateninhabers* (3.12) in einem bestimmten Kontext beitragen kann.

[QUELLE: ISO/IEC 20889:2018 [7], modifiziert]

3.23

Identität

Merkmale, die einen *Dateninhaber* (3.12) von anderen unterscheiden

3.24

indirekter Bezeichner

Attribut (3.5), das zusammen mit anderen *Attributen* (3.5), die im *Datensatz* (3.14) oder außerhalb davon sein können, eine eindeutige *Identifizierung* (3.20) eines *Dateninhabers* (3.12) innerhalb eines spezifischen Kontextes ermöglicht.

Anmerkung 1 zum Begriff: Indirekte Bezeichner können die Grundgesamtheit, zu der der *Dateninhaber* (3.12) gehört, verkleinern, und zwar bei kombinierter Verwendung unter Umständen bis auf eins. Zum Beispiel Postleitzahl, Geschlecht, Geburtsdatum.

[QUELLE: ISO/IEC 20889:2018 [7], 3.16]

3.25

Information

Wissen in Bezug auf Objekte, das innerhalb eines bestimmten Kontexts eine spezielle Bedeutung hat

[QUELLE: ISO/IEC 2382:2015 [4], 2121271]

3.26

Schlüssel

Symbolfolge, die die Operationen der *Verschlüsselung* (3.19) und der *Entschlüsselung* (3.15) steuert

[QUELLE: ISO 7498-2:1989 [10], 3.3.32]

3.27

natürliche Person

echter Mensch im Gegensatz zu einer juristischen Person, bei der es sich um eine private oder öffentliche Organisation handeln kann

3.28

Beobachtungsdaten

Daten (3.10), die von einem *Angreifer* (3.4) in einer unbefugten Weise gesammelt und verwendet werden, um *Informationen* (3.25) zu erhalten und sie einem *Dateninhaber* (3.12) zuzuordnen

3.29

Personenidentifizierung

Prozess der Herstellung einer Verbindung zwischen einem *Informationsobjekt* (3.25) und einer *natürlichen Person* (3.27)