

Anonymisierungsverfahren zur Einhaltung der DSGVO

Table of contents

1. Begriffe
2. Angriffsszenarien
3. Verfahren
 1. Suppression
 2. Generalization
 3. Maskierung
 4. Noise Addition/Distortion
 5. Shuffling/Permutation/Swapping
 6. Mikroaggregation/Clustering
4. Fazit

Begriffe

Begriffe

- personenbezogene Daten (Art. 4 I DSGVO): Alle Informationen zu einer identifizierbaren Person, besonders sensibel bei Herkunft, politischen und religiösen Ansichten oder Gesundheitsdaten.
- Datenverarbeitung (Art. 4 II DSGVO): Umfasst alle Vorgänge mit personenbezogenen Daten, z. B. Erhebung, Speicherung, Veränderung, Verwendung, ...
- Zulässigkeit der Verarbeitung (Art. 6 DSGVO): Nur erlaubt bei Einwilligung der Person oder anderen rechtlichen Grundlagen (z. B. Vertragserfüllung, rechtliche Pflicht, lebenswichtige/berechtigte/öffentliche Interessen).
- Pseudonymisierung vs. Anonymisierung

Angriffsszenarien

Angriffsszenarien

- Herausgreifen
- Verknüpfbarkeit
- Inferenz

Verfahren

Suppression

PatientID	FirstName	LastName	DateOfBirth	Gender	PhoneNumber	Address	InsuranceNumber	EmergencyContact
1	John	Doe	1985-04-12	Male	555-1234	123 Elm St, Springfield	INS12345	Jane Doe
2	Mary	Smith	1992-07-08	Female	555-5678	456 Oak St, Springfield	INS67890	Tom Smith
3	Robert	Johnson	1978-11-21	Male	555-9101	789 Pine St, Springfield	INS54321	Alice Johnson

PatientID	FirstName	LastName	DateOfBirth	Gender	PhoneNumber	Address	InsuranceNumber	EmergencyContact
1	John	Doe	1985-04-12	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Jane Doe
2	Mary	Smith	1992-07-08	Female	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Tom Smith
3	Robert	Johnson	1978-11-21	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Alice Johnson

Generalization

PatientID	FirstName	LastName	DateOfBirth	Gender	PhoneNumber	Address	InsuranceNumber	EmergencyContact
1	John	Doe	1985-04-12	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Jane Doe
2	Mary	Smith	1992-07-08	Female	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Tom Smith
3	Robert	Johnson	1978-11-21	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Alice Johnson

PatientID	FirstName	LastName	AgeGroup	Gender	PhoneNumber	Address	InsuranceNumber	EmergencyContact
1	John	Doe	30-40	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Jane Doe
2	Mary	Smith	20-30	Female	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Tom Smith
3	Robert	Johnson	40-50	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Alice Johnson

Maskierung

PatientID	FirstName	LastName	AgeGroup	Gender	PhoneNumber	Address	InsuranceNumber	EmergencyContact
1	John	Doe	30-40	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Jane Doe
2	Mary	Smith	20-30	Female	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Tom Smith
3	Robert	Johnson	40-50	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Alice Johnson

PatientID	FirstName	LastName	DateOfBirth	Gender	PhoneNumber	Address	InsuranceNumber	EmergencyContact
1	John	Doe	30-40	Male	555-XXXX	[MASKIERT]	[MASKIERT]	Jane Doe
2	Mary	Smith	20-30	Female	555-YYYY	[MASKIERT]	[MASKIERT]	Tom Smith
3	Robert	Johnson	40-50	Male	555-ZZZZ	[MASKIERT]	[MASKIERT]	Alice Johnson

Noise Addition/Distortion

PatientID	FirstName	LastName	DateOfBirth	Gender	PhoneNumber	Address	InsuranceNumber	EmergencyContact
1	John	Doe	1985-04-12	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Jane Doe
2	Mary	Smith	1992-07-08	Female	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Tom Smith
3	Robert	Johnson	1978-11-21	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Alice Johnson

PatientID	FirstName	LastName	DateOfBirth	Gender	PhoneNumber	Address	InsuranceNumber	EmergencyContact
1	John	Doe	1985-04-14	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Jane Doe
2	Mary	Smith	1992-07-10	Female	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Tom Smith
3	Robert	Johnson	1978-11-19	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Alice Johnson

Shuffling/Permutation/Swapping

PatientID	FirstName	LastName	DateOfBirth	Gender	PhoneNumber	Address	InsuranceNumber	EmergencyContact
1	John	Doe	1985-04-14	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Jane Doe
2	Mary	Smith	1992-07-10	Female	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Tom Smith
3	Robert	Johnson	1978-11-19	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Alice Johnson

PatientID	FirstName	LastName	DateOfBirth	Gender	PhoneNumber	Address	InsuranceNumber	EmergencyContact
1	Mary	Doe	1985-04-14	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Jane Doe
2	Robert	Smith	1992-07-10	Female	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Tom Smith
3	John	Johnson	1978-11-19	Male	[ENTFERNT]	[ENTFERNT]	[ENTFERNT]	Alice Johnson

Mikroaggregation/Clustering

PatientID	FirstName	LastName	DateOfBirth	Gender	PhoneNumber	Address	InsuranceNumber	EmergencyContact
1	John	Doe	1985-04-12	Male	555-1234	123 Elm St, Springfield	INS12345	Jane Doe
2	Mary	Smith	1992-07-08	Female	555-5678	456 Oak St, Springfield	INS67890	Tom Smith
3	Robert	Johnson	1978-11-21	Male	555-9101	789 Pine St, Springfield	INS54321	Alice Johnson
4	Emily	Davis	1990-05-15	Female	555-7890	101 Maple St, Springfield	INS11223	John Davis
5	Michael	Brown	1980-03-22	Male	555-2234	202 Cedar St, Springfield	INS44556	Lisa Brown
6	Sarah	Wilson	1995-10-11	Female	555-3355	303 Birch St, Springfield	INS77889	Tom Wilson

Altersgruppe	Geschlecht	Durchschnittsalter	Anzahl Patienten
20-29 Jahre	Male	27,5	2
20-29 Jahre	Female	27	1
30-39 Jahre	Male	35	3
30-39 Jahre	Female	31	1

Fazit

Fazit

- Keine universelle Lösung: Verfahren abhängig von spezifischen Anforderungen.
- Vielfältige Tools: ARX, μ -Argus, SDCMicro, Privacy Analytics Eclipse.
- Hoher manueller Aufwand: Auswahl geeigneter Verfahren und relevante Daten.
- Privacy by Design: Datenschutzmaßnahmen frühzeitig integrieren.