Kurzanleitung zum Gebrauch des Anonymisierers

Wir freuen uns, dass Sie unser Anonymisierungswerkzeug einsetzen (oder sich dafür interessieren) und damit einen Beitrag zum Datenschutz leisten.

In dieser Dokumentation finden Sie:

Diese Kurzanleitung ergänzt die integrierte Anleitung des Anonymisierers.
Sie gilt für die Versionen 2.2 und 2.3.

Bitte beachten Sie die Hinweise und Instruktionen in den Formularen (Masken) des Werkzeugs.

Installation des Anonymisierers

Der Anonymisierer ist eine MS Access-Datenbank. Er muss nicht installiert werden. Die MS Access-Datenbank kann in ein beliebiges Verzeichnis gestellt und direkt ausgeführt werden.

Im Anonymisierer werden Makros und VBA-Prozeduren ausgeführt. Setzen Sie deshalb die Sicherheitsstufe für Makros auf die niedrigste Stufe.

Bei langsamen Netzen empfehlen wir, den Anonymisierer auf einem lokalen Laufwerk auszuführen.

Vorbemerkungen

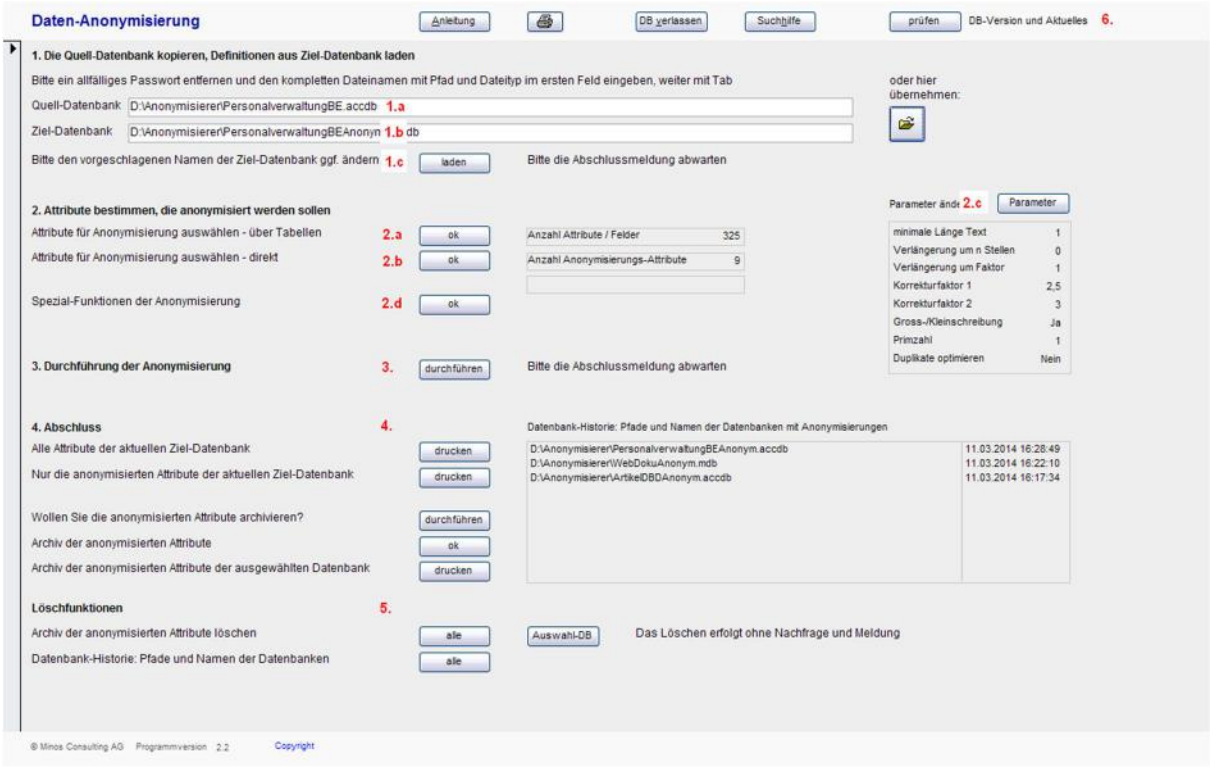
Mit wachsendem Funktionsumfang (zu Erfüllung stetig wachsender Anforderungen) wird auch die Kurzanleitung umfangreicher. Lesen Sie sie bitte trotzdem aufmerksam.

Alle Anonymisierungs-Operationen werden in einer Kopie der Datenbank durchgeführt, die die zu anonymisierenden Daten enthält. Die Originaldatenbank wird nicht verändert.

Wenn Sie Daten in Datenbanken ohne Beziehungen oder mit Beziehungen ohne referentielle Integrität und Aktualisierungsweitergabe anonymisieren, entsprechen die Ergebnisse vielleicht nicht Ihren Erwartungen.
Gleiches gilt für Datenbanken mit Tupelduplikaten.
Wir treffen solche Datenbanken in Sanierungsprojekten immer häufiger an.
Empfehlung: überarbeiten Sie Ihre Datenbanken.

Kurzanleitung zur Hauptsteuerung

Nach dem Start (Öffnen) des Anonymisierers (der Anonymisier-Datenbank) wird automatisch das Formular mit der Hauptsteuerung der Verarbeitung geöffnet:



Die Hauptverarbeitung umfasst vier Schritte (Schritte und Teilschritte sind im Bild in Rot nummeriert):

1. Quell-Datenbank kopieren, Definitionen aus Ziel-Datenbank laden
   a) Vorgabe der Quell-Datenbank, das ist diejenige Datenbank, deren Daten anonymisiert werden sollen: Entweder durch Kopieren des vollständigen Dateinamens einschliesslich des vollständigen Pfades in das Feld "Quell-Datenbank", oder durch Öffnen des Explorers mit dem Knopf rechts und Auswahl der zu anonymisierenden Datenbank durch Doppelklick.
   b) Anzeige des Namens der **Ziel-Datenbank**. Die Ziel-Datenbank ist eine Kopie der Quell-Datenbank. **In ihr wird die Anonymisierung durchgeführt**. Wenn erforderlich, kann der Name angepasst werden.
   c) Zuerst wird die Quell-Datenbank in die Ziel-Datenbank kopiert. Dann werden die Datenbank-Definitionen (der Beschreibung des Datenbank-Inhalts) aus der Ziel-Datenbank geladen.
2. Zu anonymisierende Attribute bestimmen
   a) Auswahl der zu anonymisierenden Attribute (Felder) in einem zweistufigen Formular: zuerst Tabellenauswahl, dann Attributsauswahl.
   b) Auswahl der zu anonymisierenden Attribute in einem Endlosformular mit integrierter Suchfunktion.
   Die Teil-Schritte a) und b) führen zum gleichen Ergebnis. Sie können wahlweise (a oder b) oder beide ausgeführt werden.
   c) Optional: Anpassung der Steuerungs- und Korrekturfaktoren der Anonymisierung (siehe Anleitung zur Anpassung der Parameter unten auf Seite 7).
   d) Optional: Spezialfunktionen der Anonymisierung:
      i) wiederholte Anonymisierung einer Datenbank im Laufe der Zeit, dabei werden gleiche Originalwerte immer mit dem gleichen Wert verschlüsselt
      ii) programmierte Vererbung anonymisierter Werte, für Datenbanken / Tabellen ohne Beziehungen mit RI (referentieller Integrität)
3. Durchführen der Anonymisierung der in Teil-Schritten 2.a) und / oder 2.b) ausgewählten Attribute.
4. Optional: Abschlussarbeiten

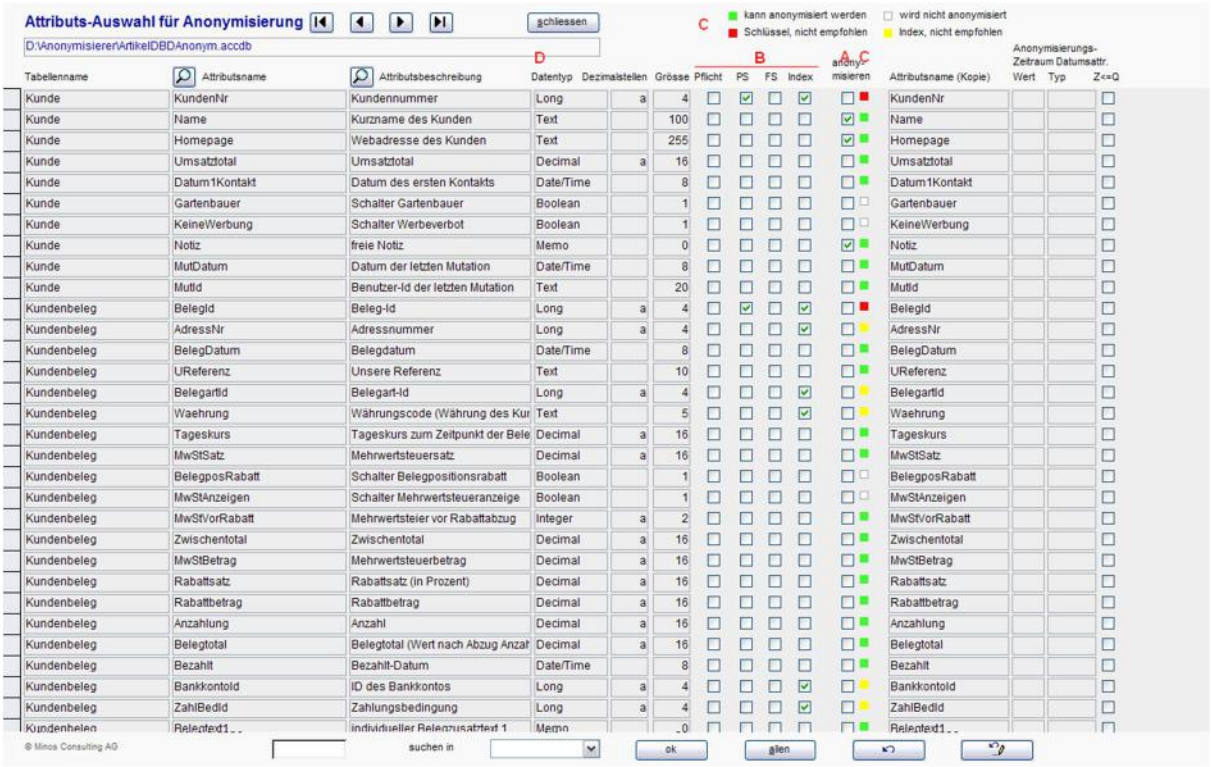
a) Drucken einer Liste aller oder nur der anonymisierten Attribute
b) Archivieren der Tabellen- und Attributs-Definitionen (-Beschreibungen) in einer Archivtabelle
c) Anzeige des Archivs in einem zweistufigen oder in einem Endlos-Formular
d) Drucken eines Berichts aller archivierten Attribute oder nur der archivierten Attribute der im Fenster rechts ausgewählten Datenbank.

5. Optional: Aufräumen:
   a) Archiv vollständig löschen
   b) Archiv für die im Fenster "Datenbank-Historie" ausgewählte Datenbank löschen
   c) Datenbank-Historie löschen.

Die im Bildschirmbild mit 6. markierte Verarbeitung ist nicht Bestandteil einer Anonymisierung. Sie kann zu beliebigen Zeiten und beliebig oft ausgeführt werden und dient
– der Prüfung der Datenbank-Version
– dem Abruf von Neuigkeiten von den Access-Experten.

Anleitung zur Attributsauswahl

Die Attributsauswahl wird am Beispiel des Endlosformulars (siehe oben Ziffer 2.b)) erläutert:

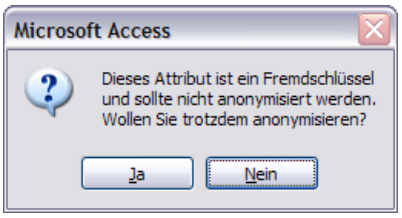
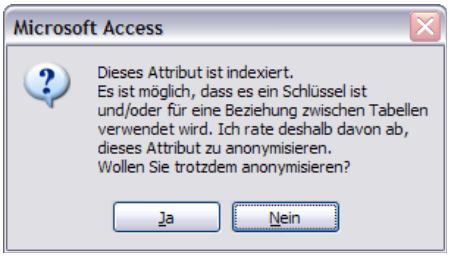
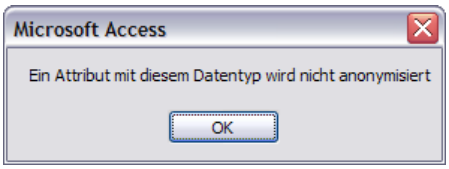


Ein Attribut wird durch Klick aufs Kontrollkästchen - siehe Buchstabe **A** - in der Spalte "anonymisieren" für das Anonymisieren ausgewählt.
Massgebend für die Anonymisierbarkeit sind:
– der Datentyp des Attributs - siehe Buchstabe **D**
– die Schlüssel- und Pflichtfeld-Eigenschaften des Attributs - siehe Bereich Buchstabe **B**.
Welche Datentypen anonymisierbar sind und welche Rolle die Schlüsseleigenschaften spielen, wird in der Anleitung (integrierte Hilfe) der Anonymisier-Datenbank erklärt.
Die zusammengefassten Regeln zur Anonymisierbarkeit werden mit farbigen Indikatoren - siehe Buchstabe **C** - visualisiert:
– "grün" heisst: das Attribut *kann* anonymisiert werden; zu möglichen Konflikten siehe unten

- "gelb" heisst: das Attribut wird in einem Index verwendet, die Anonymisierung wird nicht empfohlen
- "rot" heisst: das Attribut ist Bestandteil eines Schlüssels und sollte nicht anonymisiert werden
- "weiss" heisst: die Anonymisierung des Datentyps wird nicht unterstützt, das Attribut kann nicht anonymisiert werden.

Wird ein Attribut mit Datentyp "Datum/Uhrzeit" zur Anonymisierung ausgewählt, öffnet sich ein weiteres Fenster. Das Vorgehen wird unten auf Seite 5 erklärt.

Die wichtigsten Meldungen in der Attributsauswahl:

Meldung	Erklärung / Folgeaktion
	Die Meldung spricht für sich. Übersteuerung möglich, aber nicht empfohlen. Nur dann übersteuern, wenn RI eingeschaltet ist.
	Gleich wie oben.
	Die Anonymisierung dieses Datentyps wird nicht unterstützt.

Anleitung zur Anonymisierung von Datumsfeldern

Wird ein Attribut (ein Feld) vom Typ Datum für die Anonymisierung ausgewählt, so muss ein Zeitraum für das Ziel-Datum vorgegeben werden:
Das anonymisierte Datum - das Ziel-Datum - liegt innerhalb des Zeitraums, gerechnet ab dem Quell-Datum.

Für den Zeitraum stehen drei Einheiten zur Verfügung:
- Tag ⇨ das anonymisierte Datum ist ein beliebiger Tag innerhalb des Zeitraums
- Monat ⇨ nur der Monatswert wird anonymisiert
- Jahr ⇨ nur der Jahreswert wird anonymisiert.

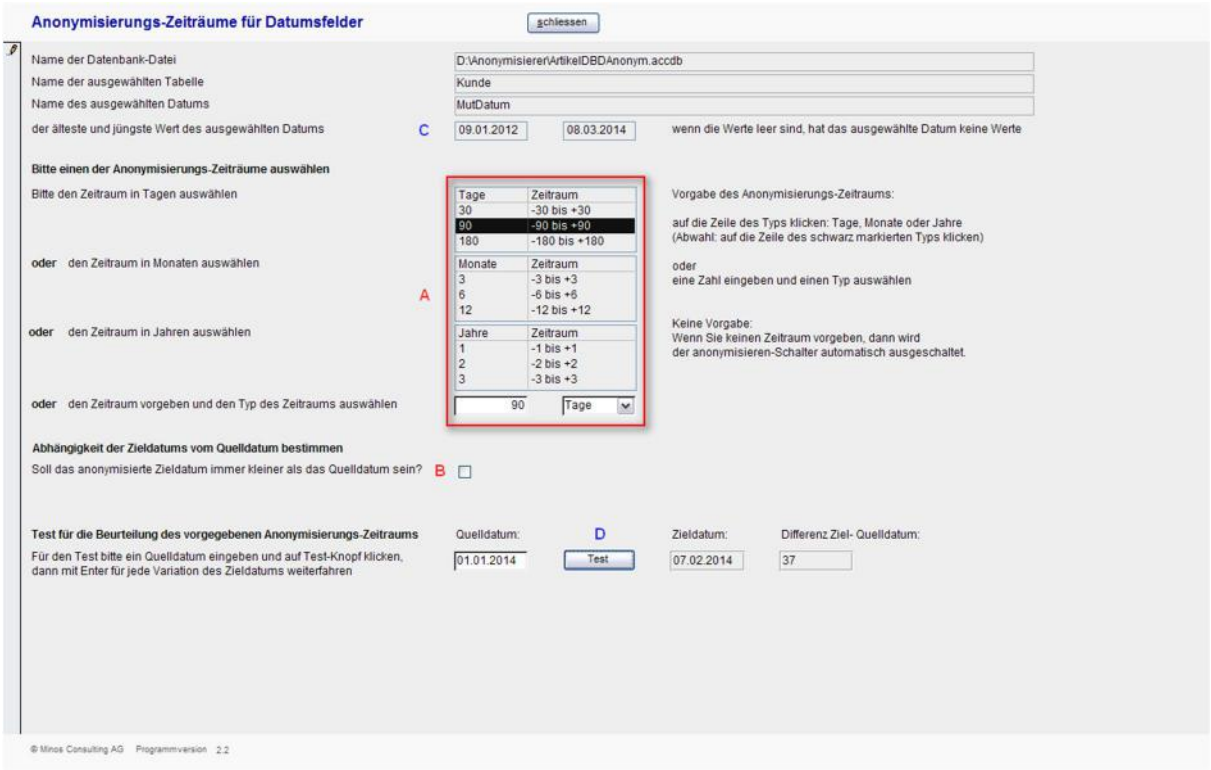
Für jede Einheit kann ein Zeitraum aus drei Standardzeiträumen ausgewählt werden - siehe Buchstabe **A** im Screenshot..

"-3 bis +3 Monate" bedeutet zum Beispiel, dass das anonymisierte Datum für den 05.11.2013 folgende Werte annehmen kann: 05.08.2013, 05.09.2013, 05.10.2013, 05.11.2013, 05.12.2013, 05.01.2014 und 05.02.2014.

Die Eigenschaften "erster Tag eines Monats / eines Jahres" und "letzter Tag eines Monats / eines Jahres" bleiben bei den Zeiträumen Monat und Jahr erhalten.

Soll das anonymisierte Datum nicht grösser (nicht jünger) als das Quelldatum sein, so ist der mit Buchstabe **B** bezeichnete Schalter zu setzen.
Diese Einschränkung ist vor allem dann sinnvoll, wenn zu anonymisierende Daten Gegenwartswerte enthalten und Datumswerte, die in der Zukunft liegen, nicht sinnvoll sind bzw. nicht verarbeitet werden können.

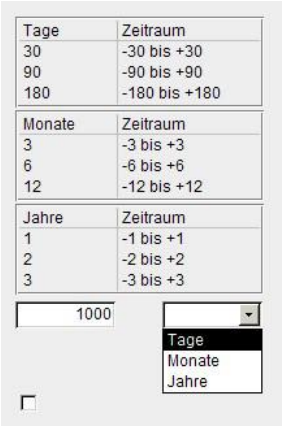
Der Wertebereich eines Datumsfelds wird zur Information in der vierten Zeile des Formulars angezeigt (im Bild mit Buchstabe **C** bezeichnetet).



Die zu erwartenden anonymisierten Datumswerte können in dem mit Buchstabe **D** bezeichneten Bereich testweise ermittelt werden.

Anstelle eines Standardzeitraums kann ein beliebiger Wert vorgegeben werden, dafür steht das Eingabefeld in der letzten Zeile des oben mit **A** bezeichneten Bereichs zur Verfügung.

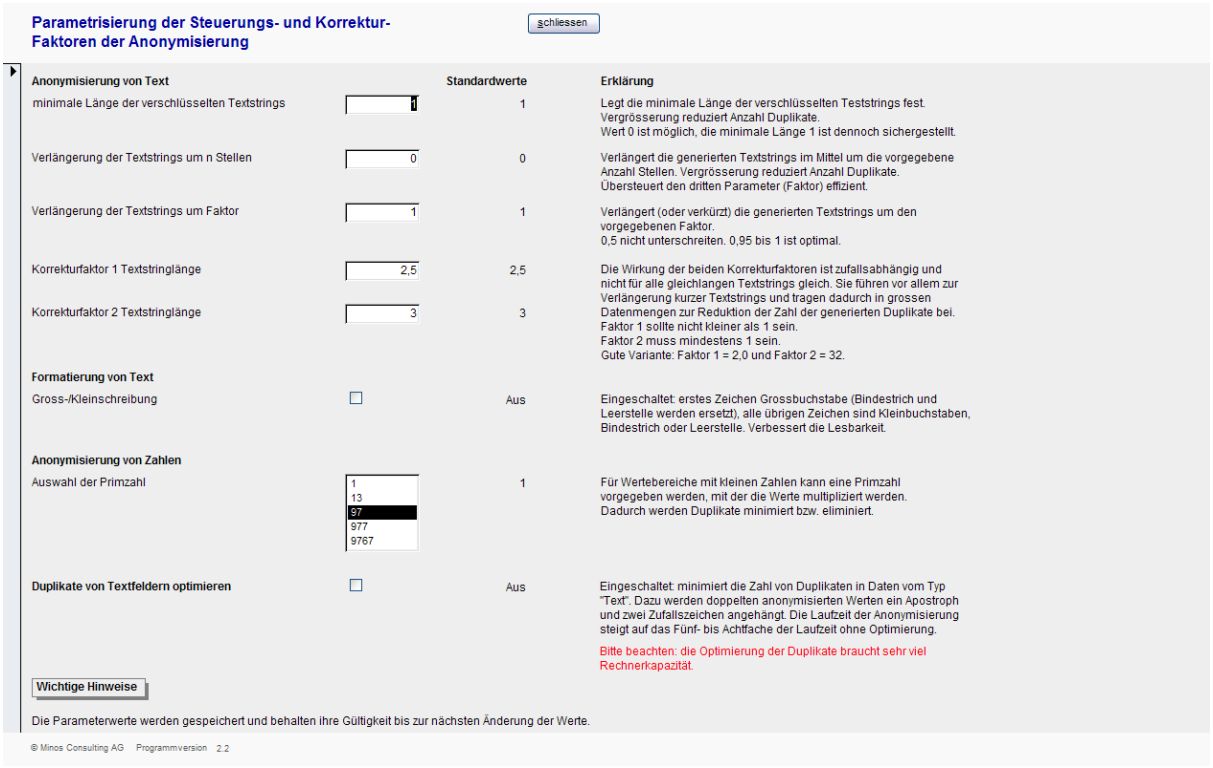
Beispiel für eine individuelle Zeitraumvorgabe:



Anleitung zur Anpassung der Parameter

Steuerungs- und Korrekturfaktoren des Anonymisierungsverfahrens für Attribute vom Typ Text können individuell angepasst werden.
Seit Anonymisierer-Version 2.2 gibt es auch einen Steuerungsfaktor für die Anonymisierung von Zahlen.

Die Standardwerte und eine ausführliche Anleitung zur Anpassung der Parameterwerte sind im Parametrisierungsformular dokumentiert:



Im Parametrisierungsformular kann auch die Formatierung anonymisierter Attribute vom Typ Text vorgegeben werden: das erste Zeichen des verschlüsselten Textstrings kann als Grossbuchstabe, alle übrigen Zeichen als Kleinbuchstabe formatiert werden.

Müssen anonymisierte Textstrings eindeutig sein, so kann der Parameter "Duplikate optimieren" gesetzt werden. Ist der Parameter gesetzt, so werden in einem zweiten Durchlauf alle mehrfach vorkommenden Textstrings ermittelt und diese um drei Stellen erweitert. Die erste Stelle der Erweiterung ist ein Apostroph, die beiden folgenden Stellen sind generierte zufällige Zeichen.
Bei grossen Datenmengen und kurzen Textstrings kann die vollständige Eliminierung von Duplikaten nicht immer erreicht werden. (Grund: aus 28 verschiedenen Zeichen können maximal 784 verschiedene zweistellige Zeichenketten generiert werden.)
In diesem zweiten Durchlauf müssen alle Tupel (Datensätze) satzweise verarbeitet werden. Diese Art der Verarbeitung benötigt sehr viel Rechnerkapazität und führt zu einer Vervielfachung der Laufzeit der Anonymisierung.

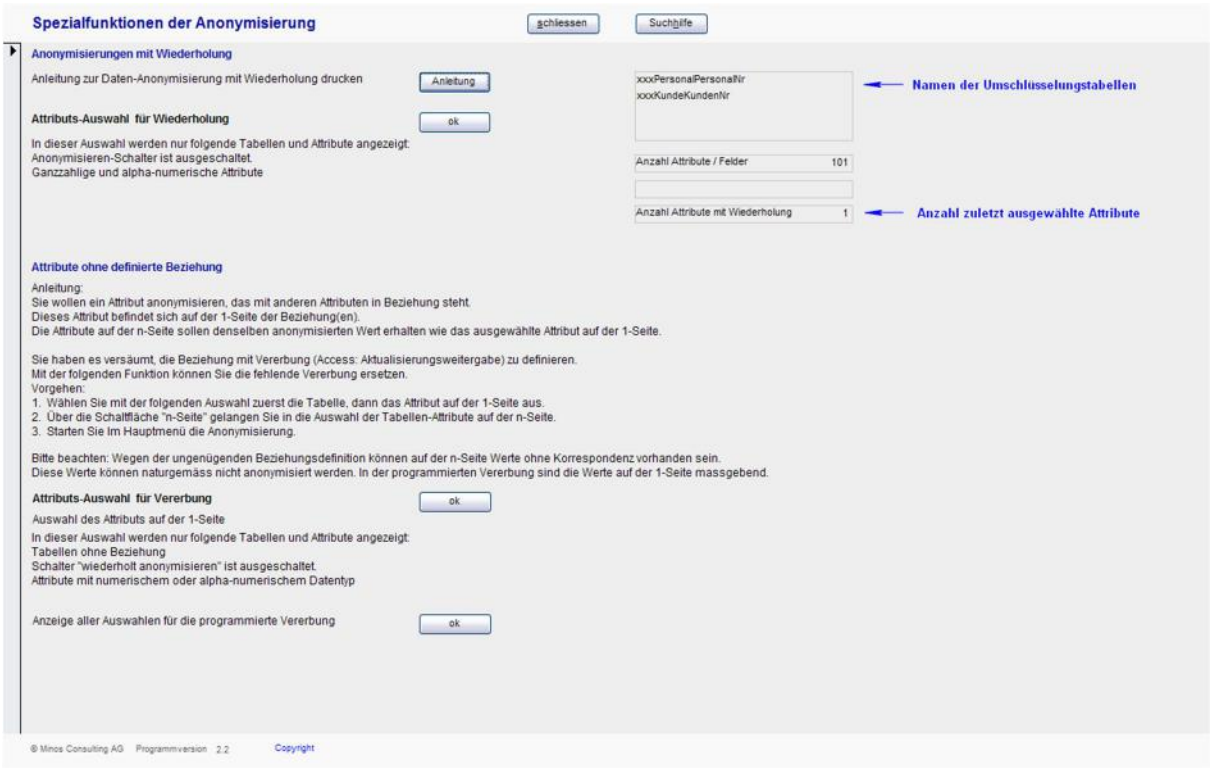
Anleitungen zu den Spezialfunktionen der Anonymisierung

Seit Version 2.2 enthält der Anonymisierer zwei Spezialfunktionen:

1. Bewahrung der Verschlüsselungswerte eines oder mehrerer Attribute bei wiederholter Anonymisierung verschiedener Versionen einer Datenbank im Laufe der Zeit. Zweck: Sicherstellen der Vergleichbarkeit von Datenauswertungen im Laufe der Zeit.
2. Programmierte Vererbung der verschlüsselten Werte eines (oder mehrerer) Attribute auf korrespondierende Attribute in anderen Tabellen der gleichen Datenbank, wenn keine datenbanktechnischen Beziehungen mit RI (referentieller Integrität) mit Aktualisierungsweitergabe zwischen den Tabellen definiert sind.

Die Auswahl der zu anonymisierenden Attribute wird in diesen beiden Fällen nicht in den Schritten 2.a) oder 2.b) in der Hauptsteuerung (siehe Kapitel "Kurzanleitung zur Hauptsteuerung" auf Seite 2) vorgenommen, sondern in den Formularen der Spezialfunktionen.

Untermenü der Spezialfunktionen:



Im oberen Bereich des Untermenüs finden Sie die erste Spezialfunktion. Bitte lesen Sie unbedingt die Anleitung zu dieser Funktion (Klick auf den Anleitungs-Knopf öffnet einen druckbaren Bericht).

Im unteren Bereich finden Sie die zweite Spezialfunktion. Beachten Sie die Anleitung. Weitere Hilfetexte finden Sie in den folgenden Formularen zur Vererbung.

Anleitung zur Spezialfunktion "wiederholte Anonymisierung"

Die Regeln und das Vorgehen entnehmen Sie bitte der Funktions-Beschreibung (in druckbarer Berichts-Form) im Spezialfunktionen-Untermenü.

Bitte beachten Sie:
- Die Namen der Tabellen und Attribute und die Struktur der Tabellen müssen in allen Wiederholungen genau gleich sein.
- Wenn Sie die Namen der wiederholt zu anonymisierenden Attribute, deren Verschlüsselungswerte bewahrt wurden, oder die Namen der Tabellen ändern, gehen die Beziehungen zu den Umschlüsselungstabellen verloren. Die Anonymisierung kann dann nicht mehr wiederholt werden.
- Die Laufzeit einer Anonymisierung mit Wiederholung ist erheblich länger als eine "normale" Anonymisierung. (Grund: Das Verfahren stellt sicher, dass die verschlüsselten Werte eindeutig sind *und* nicht in den Originalwerten vorkommen. Das benötigt Rechnerkapazität und Zeit.)

Empfehlungen:
- Erstellen Sie pro wiederholt zu anonymisierender Datenbank eine Kopie des Anonymisierers, mit dem Sie alle Wiederholungen der Versionen der Datenbank durchführen.
- Anonymisieren Sie keine anderen Datenbanken mit dieser Kopie.
- Führen Sie mit dieser Kopie keine testweisen Wiederholungen der Anonymisierung mit verschiedenen Parameterwerten für andere Attribute durch.
- Sichern Sie sowohl den Anonymisierer als auch die anonymisierte Datenbank nach jedem Anonymisierungslauf.
- Wenn Sie Primärschlüssel anonymisieren: prüfen Sie die Ergebnisse der Anonymisierung nach jedem Anonymisierungslauf - sowohl bei der erstmaligen, als auch bei den wiederholten Anonymisierungen. Falls nicht alle Primärschlüsselwerte anonymisiert wurden, nehmen Sie bitte Kontakt mit uns auf.

Tipps:
1. Sie können den Anonymisierer so oft kopieren, wie Sie wollen.
2. Sie können den Anonymisierer auch beliebig umbenennen.
3. Bevor Sie eine wiederholbare Anonymisierung durchführen, prüfen Sie zuerst mit einer "normalen" Anonymisierung die Anonymisierungsergebnisse. Wenn Sie bei kurzen Zeichenketten (wenige Zeichen lang) oder kleinen Zahlen eine Abbruchmeldung erhalten, passen Sie die Steuerungs- und Korrekturfaktoren so lange an, bis die Verschlüsselung nicht mehr abbricht. Siehe dazu Teil-Schritt 2.c) und die Anleitung auf Seite 7.
4. Wenn die Strukturen oder Attribute der Tabellen geändert werden, müssen Sie Schritt 1 ausführen und anschliessend in Schritt 2.d)i) die wiederholt zu anonymisierenden Attribute erneut auswählen.

Anleitung zur Spezialfunktion "programmierte Werte-Vererbung"

Folgen Sie der Anleitung im Spezialfunktionen-Untermenü.

Bitte beachten Sie: die programmierte Werte-Vererbung kann nur für Tabellen durchgeführt werden, welche *keine* datenbanktechnischen Beziehungen zu anderen Tabellen haben.

Erwägungen und Empfehlungen zur Anonymisierung

Der grüne Anonymisierungs-Indikator ist verführerisch und verleitet nach unserer eigenen Erfahrung dazu, mehr Attribute zu verschlüsseln, als eigentlich nötig wäre.

Anonymisieren Sie nur solche Attribute, welche schutzwürdige Daten enthalten.

Prüfen Sie, ob die Tabellen in Ihrer Datenbank über Primärschlüssel-Fremdschlüssel-Beziehungen (mit RI = referentieller Integrität) miteinander in Beziehung stehen. Ist dies nicht der Fall, prüfen Sie, welche Attribute beziehungsbildend sind. Seit Version 2.2 des Anonymisierers können Sie solche Attribute mit der Spezialfunktion "Anleitung zur Spezialfunktion "programmierte Werte-Vererbung"" (siehe Seite 9) anonymisieren und die anonymisierten Werte vererben. Beachten Sie bitte, dass inkonsistente Werte auch durch die Spezialfunktion nicht anonymisiert werden können.

Bei der Analyse Ihrer Datenbank(en) unterstützt Sie unser Analyse- und Dokumentationswerkzeug "MS Access-Datenbank-Dokumentierer". Mehr dazu finden Sie hier: www.access-experts.ch/dokumentierer .

Prüfen Sie auch, ob Ihre Datenbank **abgeleitete Attribute** enthält. Abgeleitete Attribute enthalten Werte, die aus den Werten anderer Attribute berechnet worden sind. Solche Attribute werden oft zur Leistungsverbesserung einer Datenbank angewandt.
Werden die Ausgangsattribute und / oder die zugehörigen abgeleiteten Attribute anonymisiert, so ist die Konsistenz (Widerspruchsfreiheit) der Daten verletzt. Als Folge können fehlerhafte Verarbeitungsergebnisse erzeugt werden.
Beispiele für abgeleitete Daten:

- In einer Bestellverwaltung wird der Wert einer Bestellposition aus Bestellmenge und Artikelpreis ermittelt und gespeichert: Bestellwert = Bestellmenge x Preis.
- In der Verwaltung der Jahres-Policen einer Krankenversicherung wird die Altersgruppe (Kind, Jugendlicher, Erwachsener bis 25, usw.) aus dem Geburtsdatum der versicherten Person ermittelt und gespeichert. Die Altersgruppe ist tarifbestimmend.

Prüfen Sie, ob die Ausgangsattribute und die abgeleiteten Attribute wirklich schutzwürdig sind.
Im zweiten Beispiel ist dies tatsächlich der Fall. Anonymisieren Sie in diesem Fall nur das Ausgangsattribut Geburtsdatum und führen Sie nach der Anonymisierung die Berechnung der Altersgruppe und des Versicherungstarifs (sowie der Prämie, falls diese ebenfalls gespeichert ist) gesondert durch. Gegebenenfalls müssen Sie dazu Ihre Datenbank anpassen.

Weitere Auskünfte

Access Experts
Rainer und Trudy Bauer
Steinwiesstrasse 34
8330 Pfäffikon ZH
Schweiz

Tel. +41 (0)44 950 05 60

Email: www.access-experts.ch/kontakt
Support: www.access-experts.ch/support/index.php

Web: www.access-experts.ch
www.access-experts.ch/anonymisierer
www.access-experts.ch/anonymisierer/faqs_zur_anonymisierung

Stand Dezember 2021