

# Crypto Wizard

Benutzeranleitung  
Version 2026.1.0



Hilfe zum Crypto Wizard erhalten Sie vom Datenservice:

Telefon: **+49 211 7374 1234**

E-Mail: **[datenservice@solventum.com](mailto:datenservice@solventum.com)**

## Inhaltsverzeichnis

1. Informationen zur Anwendung.....	4
1.1 Einführung .....	4
1.2 Release Notes .....	5
1.3 Systemanforderungen.....	7
2. Reduzieren und Pseudonymisieren der datenschutzrelevanten Inhalte.....	8
2.1 Daten pseudonymisieren .....	8
2.2 Daten reduzieren (§ 21-Daten).....	8
2.3 Daten reduzieren (§ 136-Daten/eQS).....	11
2.4 Daten reduzieren (SpiGes).....	11
3. Crypto Wizard ausführen.....	12
3.1 Vorbereitung .....	12
3.2 Eingangsfenster .....	13
3.3 Hauptmenü .....	13
4. Daten aufbereiten für den Versand an Solventum .....	15
4.1 § 21-Daten aufbereiten .....	16
4.2 § 136-/eQS-Daten aufbereiten .....	18
4.3 SpiGes-Daten aufbereiten.....	20
4.4 Andere Datensätze aufbereiten.....	22
4.5 Batch-Modus.....	24
4.6 Standortmapping.....	24
4.7 Konfigurationsordner anpassen .....	25
5. Ergebnisse von Solventum erhalten .....	26
5.1 Persönliches Schlüsselpaar erstellen.....	26
5.2 Hochladen des öffentlichen Schlüssels .....	28
5.3 Ergebnislieferung des Solventum Datenservice entschlüsseln.....	29
Anhang.....	31
Verschlüsselungsverfahren.....	31
Weitere Lizenzbedingungen.....	31

## 1. Informationen zur Anwendung

### 1.1 Einführung

Der Crypto Wizard ist eine Alternative zu den verfügbaren kommerziellen oder Open Source-Verschlüsselungstools mit dem Ziel, den Austausch von sensiblen Daten mit Solventum Health Information Systems mit etablierten Verschlüsselungsverfahren abzusichern. Dabei soll er in der Inbetriebnahme und im Gebrauch einfacher zu verwenden sein als die verfügbaren Alternativen.

Der Crypto Wizard wird den Kunden und Interessenten von Solventum Health Information Systems zu o. g. Zwecken kostenlos zur Verfügung gestellt.

Der Crypto Wizard beinhaltet 3 wesentliche Funktionen:

#### **Aufbereitung der Original-Daten (Reduzieren/Bereinigen und Pseudonymisieren):**

Der Crypto Wizard verändert den Original-Datensatz (Daten nach § 21 KHEntG, eQS-Daten nach § 136 SGB V sowie SpiGes-Daten), um die Anforderung der Pseudonymisierung und um das Gebot der Datensparsamkeit automatisch zu gewährleisten. Weitere Informationen dazu finden Sie im [„Reduzieren und Pseudonymisieren der datenschutzrelevanten Inhalte“](#).

#### **Verschlüsseln der Daten (Daten an Solventum versenden)**

Der Crypto Wizard ermöglicht es, Dateien zu verschlüsseln, die im Anschluss an Solventum geliefert werden sollen. Bitte finden Sie dazu weitere Informationen im Kapitel [„Daten aufbereiten für den Versand an Solventum“](#).

#### **Entschlüsseln von Daten (Daten von Solventum empfangen)**

Außerdem können Ergebnislieferungen von Solventum entschlüsselt werden. Dazu erstellt der Anwender sein eigenes asymmetrisches GPG-Schlüsselpaar. Der öffentliche Schlüssel (Dateiendung ".pub") wird im Benchmark Portal hochgeladen. Nähere Informationen erhalten Sie im Kapitel [„Ergebnisse von Solventum erhalten“](#).

## 1.2 Release Notes

### Version 2026.1.0

- Neue Benutzeroberfläche im Solventum-Design
- Datei- und Ordernamen an Solventum-Design angepasst (Achtung: auch bestehende Konfigurations- und Ausgabeordner werden umbenannt in „Crypto Wizard Konfiguration“ bzw. „Crypto Wizard Ausgabe“)
- Behebung eines Fehlers, bei dem Ordernamen für § 136-Daten und SpiGes-Daten nicht korrekt erstellt wurden
- Möglichkeit zur Definition eines abweichenden Pfads für den Konfigurationsordner implementiert

### Version 2026.0.0

- Reduzieren und Pseudonymisieren von § 21-Daten, § 136-Daten und SpiGes-Daten der Spezifikation 2026 implementiert
- Verbesserung der Verarbeitung von § 136-Daten
- Behebung eines Fehlers, bei dem Ordernamen nicht korrekt erstellt wurden
- Pfad zur Versionsabfrage wurde auf neue Solventum Domain umgestellt

### Version 2025.1.1

- Probleme beim Einlesen von fehlerhaften Eingaben innerhalb von SpiGes-Datensätzen wurden behoben
- Optimierung des Installationsordners

### Version 2025.1.0

- Pseudonymisierung und Bereinigung von SpiGes-Datensätzen (Schweiz) implementiert
- Datensatzauswahl für die Datensatzverschlüsselung überarbeitet
- Update des Java Runtime Environment (JRE) auf OpenJDK Temurin-21.0.6+7 LTS

### Version 2025.0.0

- Reduzieren und Pseudonymisieren von § 21-Daten der Spezifikation 2025 implementiert
- Bereinigung von § 136-Daten der Spezifikation 2025 implementiert
- Generierung des persönlichen GPG-Schlüsselpaars jetzt als RSA-Schlüssel mit 4096 Bit Länge

### Version 2024.1.0

- Funktion zum Standortmapping bei der Verarbeitung von § 136-Daten implementiert; nähere Informationen dazu erhalten Sie im [„Standortmapping“](#)
- Neue Datensatzspezifikation für § 21-Daten umgesetzt

### Version 2024.0.1

- Probleme beim Abruf der Versionsinformationen vom Server 3mhisdataservices.com (durch neue Zertifizierungsstelle im Serverzertifikat) wurden behoben

### Version 2024.0.0

- Bereinigung von § 136-Daten der Spezifikation 2024 implementiert
- Reduzieren und Pseudonymisieren von § 21-Daten bleibt für 2024 unverändert
- Speicherung der Logdateien jetzt im Konfigurationsordner „3M CryptoWizard Konfiguration“ im persönlichen Dokumentenordner („Eigene Dateien“ bzw. „Dokumente“) statt wie bisher im Unterordner „Log“ im Programmordner des CryptoWizard

Version 2023.0.1

- Umstellung der Bezeichnung von „§ 137“ bzw. „P137“ nach „§ 136“ bzw. „P136“ in der Benutzeroberfläche und in Ordner-/Dateinamen der Ausgabe
- Fehlerbehebung bei der Bestimmung von IK und Datenjahr und entsprechender Benennung von Ordner-/Dateinamen in der Ausgabe bei § 136-Daten
- § 21-Standortmapping: erweitert um das Feld „Standortnummer-Behandlungsort“
- Batch-Modus: Parameter „P137“ geändert nach „P136“

Version 2023.0.0

- Bereinigung von § 136-Daten der Spezifikation 2023 implementiert
- Java Runtime Environment auf OpenJDK 17 JRE aktualisiert
- Funktion zum Standortmapping bei der Verarbeitung von § 21-Daten implementiert; nähere Informationen dazu erhalten Sie im Kapitel [„Standortmapping“](#)

Version 2022.0.0

- Bereinigung von § 136-Daten der Spezifikation 2022 implementiert
- Batch-Funktionalität zur Verarbeitung und Verschlüsselung mehrerer Datensätze ohne Benutzeroberfläche implementiert

Version 2021.0.0

- Bereinigung von § 136-Daten der Spezifikation 2021 implementiert

Version 2020.1.2

- Fehler beim Start des CryptoWizard behoben, der bei fehlender Internetverbindung auftrat und die normale Nutzung verhinderte

Version 2020.1.1

- Performance und Stabilität beim Reduzieren und Pseudonymisieren von § 21-Daten verbessert
- Stabilität bei der Bereinigung von § 136-Daten verbessert
- Transparenz des Verarbeitungsprozesses verbessert durch detaillierte Informationen zum Umfang und Stand der Verarbeitung

Version 2020.0.0

- Reduzieren und Pseudonymisieren von § 21-Daten nach Datensatzbeschreibung 2020 implementiert
- Bereinigung von § 136-Daten der Spezifikation 2020 implementiert
- Funktion zur Benachrichtigung des Benutzers, falls eine neuere Version des CryptoWizard zum Download bereitsteht
- Funktion zur Verschlüsselung „anderer“ Datensatzformate wurde überarbeitet, so dass jede ausgewählte Datei zu jeweils einer separaten Datenlieferung (GPG-Datei) verschlüsselt wird. Nähere Informationen im Abschnitt [„Andere Datensätze aufbereiten“](#).
- Verbesserte Stabilität bei der Generierung von Schlüsselpaaren

Version 2019.0.2

- Verbessertes Management der Konfigurationsdateien
- Verbesserte Stabilität bei Schlüsselgenerierung und Entschlüsselung
- Kleine Verbesserungen der Benutzeroberfläche und der Logdateien

Version 2019.0.1

- Bereinigung von § 136-Daten der Spezifikation 2019 implementiert
- Verbesserungen bei der Validierung von § 21- sowie § 136-Datenlieferungen

Version 3.1.3

- Fehler beim Aufbau der Mappingdatei (§ 21-Daten) behoben, bei dem u. U. unkorrekte Werte für den Standort sowie das Entlassungsjahr gespeichert wurden
- Fehler bei der Reduzierung von § 21-Daten behoben, bei dem u. U. IK-Felder sowie Belegungstage nicht wie vorgesehen reduziert wurden
- Kleinere Verbesserungen bei der Validierung von § 21- sowie § 136-Datenlieferungen

Version 3.1.2

- Berücksichtigung der neuen Felder zur Intensivbehandlung in den Dateien FALL und FAB des § 21-Datensatzes zur Lieferung in 2019
- Kleinere Verbesserungen bei der Validierung von § 21- sowie § 136-Datenlieferungen

Version 3.1.1

- Verbesserung der Stabilität bei der Ver- und Entschlüsselung
- Erzeugung von ungültigen Zeichen bei der Bereinigung von XML-Dateien (§ 136-Daten) mit vom XML-Zeichensatz (UTF-8) abweichenden Zeichenkodierungen behoben

Version 3.1

- Ergänzung der automatischen Funktion "PID-Inhalte entfernen" für § 136-Daten
- Fehler bei der Reduzierung von ICD-Dateien (§ 21-Daten) mit UTF-8 Zeichenkodierungen behoben

Version 3.0

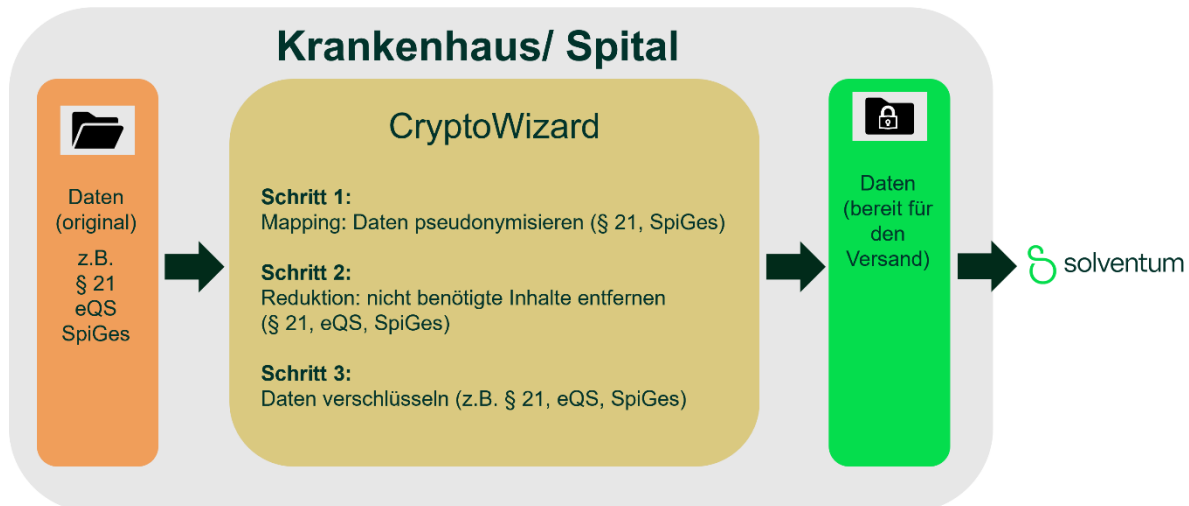
- Ergänzung der automatischen Funktion "Pseudonymisieren" für § 21-Daten
- Ergänzung der automatischen Funktion "Reduzieren" für § 21-Daten
- Optimierte Ablage der Ergebnisdateien

**1.3 Systemanforderungen**

- Betriebssystem: Windows 10, Windows 11
- Administrator-Berechtigungen nicht erforderlich (keine Installation)
- Vollzugriff auf Ordner für persönliche Dokumente („Eigene Dateien“, „Eigene Dokumente“, Bibliothek „Dokumente“ o.ä.)
- Ausführbarkeit von Java-Anwendungen (das erforderliche Java Runtime Environment OpenJDK 21 JRE wird mitgeliefert)
- Möglichkeit zum Entpacken von ZIP-Archiven

## 2. Reduzieren und Pseudonymisieren der datenschutzrelevanten Inhalte

Der Crypto Wizard wurde gezielt weiterentwickelt, um eine datenschutzkonforme Übertragung von Krankenhausroutinedaten im Rahmen einer Auftragsdatenverarbeitung zu gewährleisten. Das Prinzip: die Original-Daten werden (je nach Datensatz) vor Übertragung an Solventum mit dem Crypto Wizard pseudonymisiert, reduziert und anschließend verschlüsselt. Die verschlüsselte Ergebnisdatei kann dann an Solventum übergeben werden.



### 2.1 Daten pseudonymisieren

Bei der Aufbereitung der § 21- und SpiGes-Daten führt der Crypto Wizard ein automatisches Mapping der Fallnummern durch. Dabei wird die Original-Fallnummer gegen ein Pseudonym ausgetauscht. Gleichzeitig wird bei diesem Vorgang eine Mappingdatei erzeugt, die im Krankenhaus verbleibt und später eine Rückübersetzung vom Pseudonym zur Original-Fallnummer ermöglicht. Bitte beachten Sie dazu folgenden Hinweis:

**Bitte laden Sie immer einen § 21- Datensatz mit originalen (Krankenhaus-internen) Fallnummern in den Crypto Wizard. Nutzen Sie bitte zuvor **keine** weitere Pseudonymisieren-Funktion (z. B. über die Export-Schnittstelle oder ein anderes Tool zur Pseudonymisierung). Andernfalls ist keine Rückübersetzung zur Original-Fallnummer gewährleistet. Das gleiche gilt auch für den SpiGes-Datensatz.**

### 2.2 Daten reduzieren (§ 21-Daten)

In diesem Arbeitsschritt entfernt der Crypto Wizard alle Inhalte des § 21-Datensatzes, die nicht zur Ergebnisberechnung erforderlich sind. Das Tool berücksichtigt grundsätzlich nur die § 21-Dateien „FALL“, „FAB“, „ICD“, „OPS“ und „ENTGELTE“ in allen standardisierten Ausprägungen und aktuellen Versionen. Weitere Dateien bleiben unberücksichtigt und werden nicht mit verschlüsselt.

Innerhalb der Dateien werden die Inhalte bestimmter Datenfelder entweder ganz entfernt oder soweit reduziert bzw. verändert, dass kein Rückschluss auf den Original-Inhalt möglich ist. Die folgende Tabelle gibt Ihnen eine Übersicht der Veränderungen:

Alle hier nicht aufgeführten Felder bleiben unverändert. Felder, die nicht Teil einer § 21-Datensatzspezifikation sind, werden vollständig entfernt.



<b>Datei § 21</b>	<b>Datenfeld</b>	<b>Operation im Normalbetrieb</b>	<b>Operation im Modus "Verwendung für Leistungsanalysen"</b>
FALL	KH-internes-Kennzeichen	Austausch der Original-Fallnummer gegen Pseudonym	Austausch der Original-Fallnummer gegen Pseudonym
FALL	Versicherten-ID	Inhalt wird entfernt	Inhalt wird entfernt
FALL	Vertragskennzeichen-64b-Modellvorhaben	Inhalt wird entfernt	Inhalt wird entfernt
FALL	IK-der-Krankenkasse	Inhalt wird reduziert (Übernahme der ersten beiden Stellen, dann folgen "0000000")	Inhalt wird reduziert (Übernahme der ersten beiden Stellen, dann folgen "0000000")
FALL	Geburtsmonat	Inhalt wird entfernt	Inhalt wird entfernt
FALL	PLZ	Inhalt wird entfernt	Inhalt wird entfernt
FALL	Aufnahmegewicht	Inhalt wird verändert (Wert wird in 25er-Schritten gerundet)	Inhalt wird verändert (Wert wird in 25er-Schritten gerundet)
FALL	Patientennummer	Austausch der Original-Patientennummer gegen Pseudonym	Austausch der Original-Patientennummer gegen Pseudonym
FALL	Behandlungsbeginn-vorstationär	Inhalt wird entfernt	Inhalt wird entfernt
FALL	Behandlungstage-vorstationär	Inhalt wird entfernt	Inhalt wird entfernt
FALL	Behandlungsende-nachstationär	Inhalt wird entfernt	Inhalt wird entfernt
FALL	Behandlungstage-nachstationär	Inhalt wird entfernt	Inhalt wird entfernt
FALL	IK-Verlegungs-KH	Inhalt wird entfernt	Inhalt wird entfernt
FALL	Belegungstage-in-anderem-Entgeltbereich	Inhalt wird entfernt	Inhalt wird entfernt
FALL	Felder, die nicht in der § 21-Datensatzbeschreibung definiert sind (z. B. zusätzliche Felder im § 21Plus-Datensatz)	Inhalt wird entfernt	Inhalt wird entfernt
FAB	KH-internes-Kennzeichen	Austausch der Original-Fallnummer gegen Pseudonym	Austausch der Original-Fallnummer gegen Pseudonym
FAB	Felder, die nicht in der § 21-Datensatzbeschreibung definiert sind (z. B. zusätzliche Felder im § 21Plus-Datensatz)	Inhalt wird entfernt	Inhalte mit Fachabteilungsinformationen/Stationen bleiben erhalten
ICD	KH-internes-Kennzeichen	Austausch der Original-Fallnummer gegen Pseudonym	Austausch der Original-Fallnummer gegen Pseudonym

<b>Datei § 21</b>	<b>Datenfeld</b>	<b>Operation im Normalbetrieb</b>	<b>Operation im Modus "Verwendung für Leistungsanalysen"</b>
ICD	Diagnosensicherheit	Inhalt wird entfernt	Inhalt wird entfernt
ICD	Felder, die nicht in der § 21-Datensatzbeschreibung definiert sind (z. B. zusätzliche Felder im § 21Plus-Datensatz)	Inhalt wird entfernt	Inhalt wird entfernt
OPS	KH-internes-Kennzeichen	Austausch der Original- Fallnummer gegen Pseudonym	Austausch der Original- Fallnummer gegen Pseudonym
OPS	Felder, die nicht in der § 21- Datensatzbeschreibung definiert sind (z. B. zusätzliche Felder im § 21Plus-Datensatz)	Inhalt wird entfernt	Inhalt wird entfernt
Entgelte	KH-internes-Kennzeichen	Austausch der Original- Fallnummer gegen Pseudonym	Austausch der Original- Fallnummer gegen Pseudonym
Entgelte	IK-Krankenkasse	Inhalt wird reduziert (Übernahme der ersten beiden Stellen, dann folgen "0000000")	Inhalt wird reduziert (Übernahme der ersten beiden Stellen, dann folgen "0000000")
Entgelte	Entgeltart	mit 4 beginnend gelöscht	bleibt
Entgelte	Entgeltbetrag	auf 0 gesetzt	bleibt
Entgelte	Abrechnung-von	Inhalt wird entfernt	Inhalt wird entfernt
Entgelte	Abrechnung-bis	Inhalt wird entfernt	Inhalt wird entfernt
Entgelte	Tag-der-Behandlung	Inhalt wird entfernt	Inhalt wird entfernt
Entgelte	Felder, die nicht in der § 21-Datensatzbeschreibung definiert sind (z. B. zusätzliche Felder im § 21Plus-Datensatz)	Inhalt wird entfernt	Inhalt wird entfernt

### 2.3 Daten reduzieren (§ 136-Daten/eQS)

Sofern Sie Daten der externen Qualitätssicherung nach § 136 SGB V (eQS-Daten) zur Abgabe an den Datenservice aufbereiten möchten, entfernt der Crypto Wizard aus Datenschutzgründen alle Patientenidentifizierenden Merkmale (PID-Infos) aus den Dateien. Alle zusätzlichen Felder, d.h. Felder, die nicht als Exportfelder in der Spezifikation des IQTiG vorgesehen sind, werden ebenfalls geleert. Zur Aufbereitung können Sie sowohl XML- als auch CSV- bzw. Textdateien mit dem Crypto Wizard aufbereiten.

**Achtung: das IQTiG überarbeitet jährlich die Spezifikationen der eQS-Daten. Bitte überprüfen Sie daher vor Aufbereitung der Daten, ob Sie die neueste Version des Crypto Wizard einsetzen.**

### 2.4 Daten reduzieren (SpiGes)

In diesem Arbeitsschritt entfernt der Crypto Wizard alle Inhalte des SpiGes-Datensatzes, die nicht zur Ergebnisberechnung erforderlich sind und aufgrund des Gebots der Datensparsamkeit oder aus datenschutzrechtlichen Gründen nicht an Solventum geliefert werden dürfen.

Das Tool berücksichtigt grundsätzlich nur die SpiGes XML Datendatei. Diese enthält Diagnosen, Behandlungen, Eintrittsdatum, Alter und weitere für die Qualitätsauswertungen relevante fallbezogene Informationen. Die SpiGes XML Identifikatorendatei mit den AHV-Nummern bleibt unberücksichtigt und wird nicht mit verschlüsselt.

Innerhalb der berücksichtigten SpiGes XML Datendatei werden die Inhalte der Datenfelder (Variablen) unverändert gelassen, gänzlich entfernt oder so weit verändert, dass möglichst kein Rückschluss auf den Original-Fall möglich ist.

**Die folgende Auflistung gibt Ihnen eine Übersicht der vom Crypto Wizard unverändert gelassenen Feldwerte:**

"episode\_id", "episode\_beginn", "episode\_ende", "episode\_art", "burnr\_episode",  
 "grund\_wiedereintritt", "wiedereintritt\_aufenthalt", "ent\_id", "uid", "alter\_U1", "chlz", "burnr", "tarif",  
 "aufwand\_imc", "aufenthalt\_imc", "nems", "art\_score", "schwere\_score", "beatmung",  
 "austritt\_behandlung", "austritt\_aufenthalt", "austrittsentscheid", "austrittsdatum",  
 "hauptleistungsstelle", "admin\_urlaub", "aufenthalt\_ips", "einw\_instanz", "eintrittsart",  
 "eintritt\_aufenthalt", "eintrittsdatum", "alter", "geschlecht", "splg", "vitalstatus", "diagnose\_id",  
 "diagnose\_poa", "diagnose\_zusatz", "diagnose\_seitigkeit", "diagnose\_kode", "behandlung\_id",  
 "behandlung\_auswaerts", "behandlung\_seitigkeit", "behandlung\_chop", "behandlung\_beginn",  
 "behandlung\_bur"

**Folgende Feldwerte werden transformiert (auf- oder abgerundet):**

"aufnahmegewicht", "geburtsgewicht"

**Folgender Feldwert wird pseudonymisiert:**

"fall\_id"

Alle hier nicht aufgeführten Felder werden vollständig geleert.

### 3. Crypto Wizard ausführen

#### 3.1 Vorbereitung

Laden Sie den Crypto Wizard über den Link, den Sie von Solventum erhalten haben, herunter. Speichern Sie das ZIP-Archiv in einem Ordner auf den Vollzugriff besteht, wie z. B. Ihren persönlichen Dokumentenordner oder Desktop.

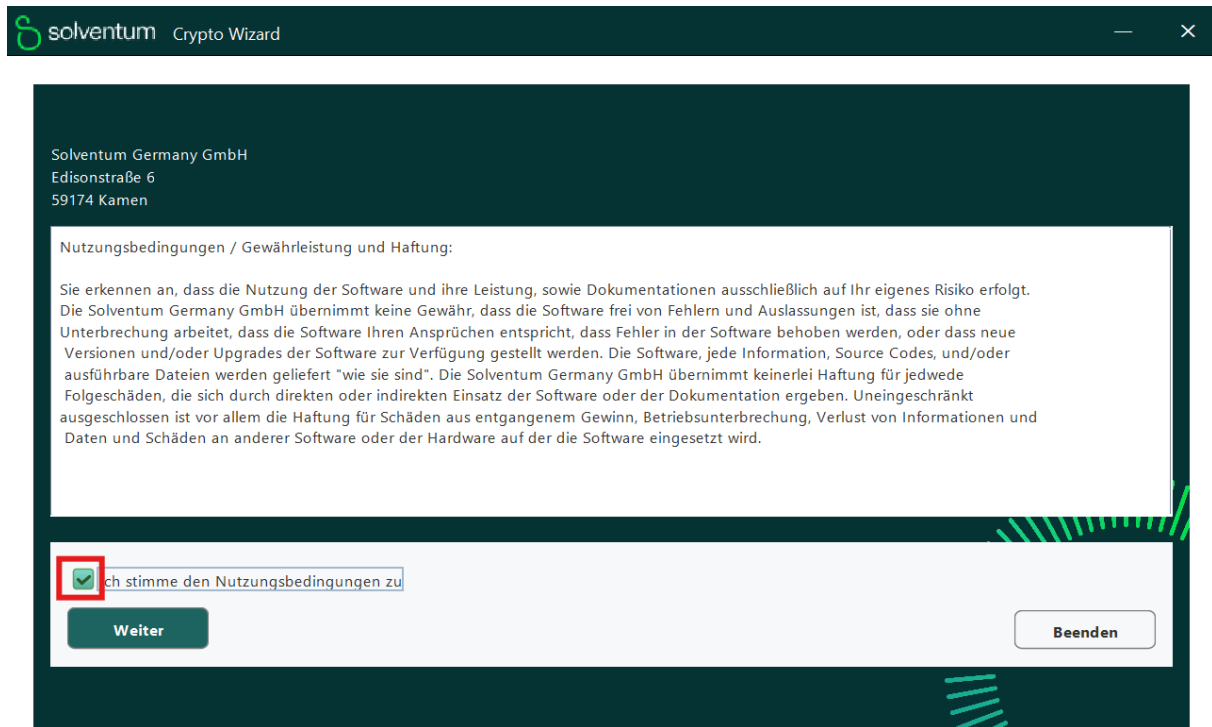
Eine Installation des Crypto Wizard ist nicht erforderlich. **Das heruntergeladene ZIP-Archiv (SolventumCryptoWizard.zip) muss lediglich vor dem Starten vollständig entpackt werden.** Alle zur Ausführung benötigten Ressourcen werden mitgeliefert.

Entpacken Sie das ZIP-Archiv mit Hilfe eines geeigneten Tools oder mit Windows-Bordmitteln vollständig in einen Unterordner, indem Sie mit der rechten Maustaste auf das ZIP-Archiv klicken und den Befehl „Alle extrahieren...“ ausführen.

Name	Status	Änderungsdatum	Typ	Größe
config	✓	20.03.2026 15:29	Dateiordner	
doc	✓	20.03.2026 15:29	Dateiordner	
GnuPG	✓	20.03.2026 15:29	Dateiordner	
jre	✓	20.03.2026 15:29	Dateiordner	
misc	✓	20.03.2026 15:29	Dateiordner	
BatchBeispiel.bat	✓	04.03.2026 14:12	Windows-Batchda...	1 KB
<b>CryptoWizard.exe</b>	✓	18.03.2026 13:46	Anwendung	539 KB
CryptoWizard.jar	✓	19.03.2026 17:29	JAR-Datei	18.969 KB
CryptoWizardBatch.exe	✓	18.03.2026 13:46	Anwendung	496 KB
CryptoWizardBatch.jar	✓	18.03.2026 13:39	JAR-Datei	18.361 KB
jmap2.dll	✓	20.09.2024 11:53	Anwendungserwei...	376 KB

Starten Sie die im Unterordner enthaltene Anwendungsdatei „CryptoWizard.exe“ per Doppelklick.

### 3.2 Eingangsfenster



Im Eingangsfenster des Crypto Wizard sind die Nutzungsbedingungen abgebildet. Um zur nächsten Seite zu gelangen, müssen Sie diesen zustimmen und auf **Weiter** klicken.

Sofern Sie den Crypto Wizard beenden möchten, klicken Sie auf **Beenden**.

### 3.3 Hauptmenü

Im Hauptmenü können Sie alle Funktionalitäten des Crypto Wizard anwählen. Welche Funktion für Sie gerade relevant ist, ergibt sich aus der Einteilung in die 2 Rubriken „Daten an Solventum senden“ sowie „Ergebnisse von Solventum erhalten“.



Sollte eine neuere Version des Crypto Wizard zum Download bereitstehen, erhalten Sie oberhalb des Hauptmenüs einen entsprechenden Hinweis. In diesem Fall können Sie direkt auf den angezeigten Link klicken, um die neue Version herunterzuladen.

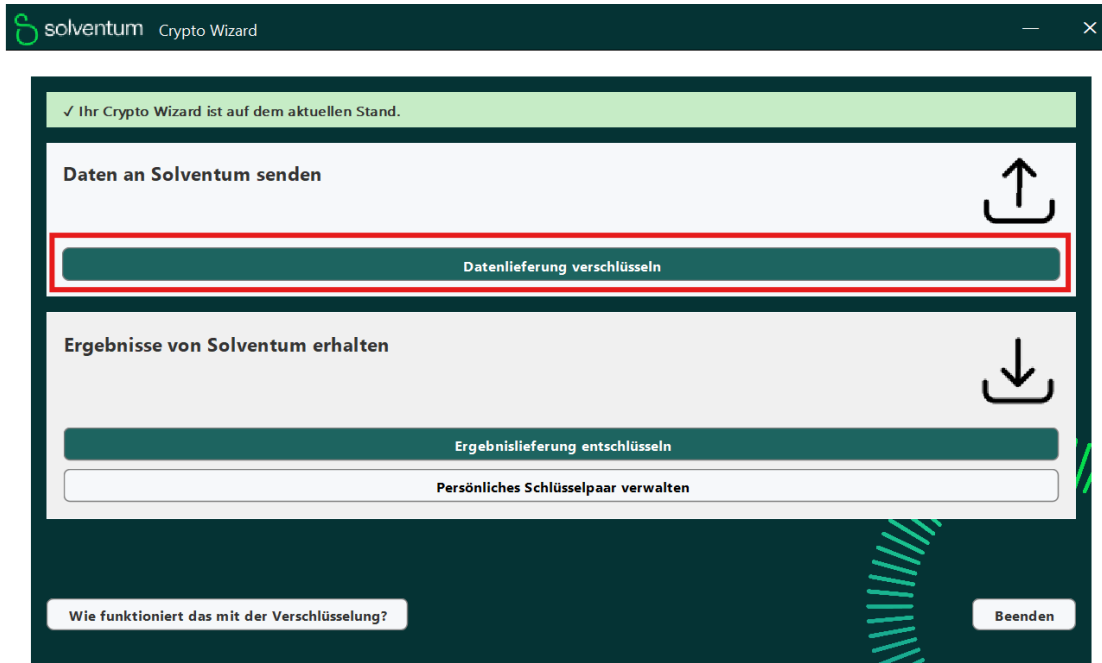
Ist jedoch die von Ihnen verwendete Version die neueste, wird auch das oberhalb des Hauptmenüs angezeigt:

✓ Ihr Crypto Wizard ist auf dem aktuellen Stand.

#### 4. Daten aufbereiten für den Versand an Solventum

Unter dem Punkt „Daten an Solventum senden“ werden die Dateien aufbereitet und mit Hilfe des öffentlichen Schlüssels von Solventum verschlüsselt, um sie danach im Benchmark Portal hochladen zu können. Im Crypto Wizard ist der richtige Schlüssel des Solventum Datenservice bereits hinterlegt.

Wählen Sie den Punkt „Datenlieferung verschlüsseln“.



Wählen Sie in der folgenden Ansicht zunächst die Datensatzart aus. Sie können „§ 21 Daten“, „§ 136 Daten“, „SpiGes Daten“ oder „Andere Datensatzformate“ wählen.

Unter „Andere Datensatzformate“ fallen alle Dateiformate, die nicht zu den § 21-Daten, § 136-/eQS-Daten und SpiGes-Daten gehören (z. B. spezielle Falldaten-Formate).

#### 4.1 § 21-Daten aufbereiten

solventum Crypto Wizard

Bitte wählen Sie, welche Art von Datensatz Sie verschlüsseln möchten:

§ 21 Daten (inkl. Pseudonymisierung)

Hier Auswahl treffen...

§ 21 Daten (inkl. Pseudonymisierung)

§ 136 Daten (inkl. PID-Bereinigung)

SpiGes Daten (inkl. Pseudonymisierung)

Andere Datensatzformate

+ Durchsuchen...

☒ Verwendung für Leistungsanalysen (Alle Informationen zu Entgelten und Stationen bleiben erhalten)

Pseudonymisieren & Verschlüsseln

**Hinweis:**  
Sie können hier einen oder mehrere Ordner oder schon komprimierte Dateien (Endung .zip, .7z oder .rar) mit jeweils einem vollständigen § 21-Datensatz auswählen.

Zurück zum Hauptmenü

solventum Crypto Wizard

Bitte wählen Sie, welche Art von Datensatz Sie verschlüsseln möchten:

§ 21 Daten (inkl. Pseudonymisierung)

Bitte wählen Sie einen oder mehrere Ordner mit je einem zu verschlüsselnden Datensatz:

+ Durchsuchen...

☒ Ausgabe im Standard-Ausgabeordner

☒ Verwendung für Leistungsanalysen (Alle Informationen zu Entgelten und Stationen bleiben erhalten)

Pseudonymisieren & Verschlüsseln

**Hinweis:**  
Sie können hier einen oder mehrere Ordner oder schon komprimierte Dateien (Endung .zip, .7z oder .rar) mit jeweils einem vollständigen § 21-Datensatz auswählen.

Zurück zum Hauptmenü

Wählen Sie zunächst die Datensatzart „§ 21 Daten“ aus.

**Bitte achten Sie bei § 21-Daten unbedingt darauf, dass die Fallnummern in den Dateien **nicht** bereits zuvor eine andere Pseudonymisieren-Funktion durchlaufen haben (z. B. beim Export über die KIS-Schnittstelle oder ein anderes Tool zur Pseudonymisierung).**



Um einen oder mehrere Datensatz/Datensätze auszuwählen, klicken Sie bitte auf

+ Durchsuchen...

Im folgenden Dialog wählen Sie bitte **Ordner** mit je einem vollständigen § 21-Datensatz aus. Mehrere Ordner können durch Halten der Strg-Taste und Anklicken einzelner Ordner ausgewählt werden. Alternativ können hier auch ZIP-Archivdateien ausgewählt werden, die jeweils einen vollständigen § 21-Datensatz enthalten müssen.

Die Ausgabeordner werden dann im Normalfall am selben Ort abgelegt, an dem auch die Eingabeordner gespeichert sind. Alternativ können Sie die Option

☒ Ausgabe im Standard-Ausgabeordner

durch Setzen des Hakens aktivieren. Die Ausgabeordner werden dann im Ordner „Crypto Wizard Ausgabe“ in Ihrem persönlichen Dokumentenordner abgelegt. Wo genau dieser Ordner auf Ihrem System zu finden ist, wird Ihnen in einem Tooltip angezeigt. Halten Sie dazu den Mauszeiger etwas länger über die Checkbox.

Die Option

☐ Verwendung für Leistungsanalysen (Alle Informationen zu Entgelten und Stationen bleiben erhalten)

wählen Sie bitte nur dann aus, wenn Sie die Daten zur Verwendung für Leistungsanalysen zusenden möchten.

Um die Aufbereitung der Daten zu starten, klicken Sie auf

Pseudonymisieren & Verschlüsseln

Bitte beachten Sie, dass bei großen § 21-Datensätzen (oder mehreren gleichzeitig zur Verarbeitung ausgewählten Datensätzen) mit langen Laufzeiten zu rechnen ist, da Änderungen in mehreren Millionen Zeilen vorgenommen werden müssen. Befindet sich zudem der Speicherort der Eingabedaten und/oder der Ausgabedaten auf einem Netzlaufwerk, verlängert sich die Laufzeit entsprechend, da die Daten über das Netzwerk geladen werden müssen.

**Richtwert: 5 Minuten Laufzeit / 20.000 Fälle.**

Nach Abschluss der Verarbeitung legt der Crypto Wizard im Zielordner pro Datensatz je einen Ausgabeordner (benannt mit „P21\_“, Institutionskennzeichen, Datenjahr, Name des gewählten Originalordners) und folgendem Inhalt an:

Mappingdatei

Original

Pseudonymisiert

P21\_232323232\_2024\_63054446742139.zip.gpg

Im Ordner „Mappingdatei“ finden Sie die Mappingdatei (benannt mit „Mappingdatei\_“, Institutionskennzeichen, Datenjahr, Erstellungsdatum und Uhrzeit).

Über diese Datei kann ein direkter Bezug zwischen der Original-Fallnummer und dem im Datensatz eingesetzten Pseudonym hergestellt werden. **Bitte senden Sie diese Datei niemals an Solventum.** Sie benötigen diese Datei später, um in fallbezogenen Ergebnissen, die Sie von Solventum erhalten, einen Bezug zur Original-Fallnummer herstellen zu können. **Bitte bewahren Sie diese Datei daher an einem sicheren Speicherort auf.**

Im Ordner „Original“ finden Sie den Original-Datensatz als ZIP-Archiv. Über diese Datei können Sie zu einem späteren Zeitpunkt genau nachvollziehen, welche Datengrundlage für die Datenaufbereitung verwendet wurde.

Im Ordner „Pseudonymisiert“ finden Sie den erzeugten Datensatz (pseudonymisiert und reduziert, siehe Kapitel 2) als ZIP-Archiv. Über diese Datei können Sie das Ergebnis der Datenaufbereitung nachvollziehen.

Neben diesen drei Ordnern finden Sie auch die fertig verschlüsselte GPG-Datei (benannt mit „P21\_“, Institutionskennzeichen, Datenjahr und einem Zahlencode).

Diese Datei, welche den pseudonymisierten Datensatz enthält, ist mit dem Solventum-Datenservice-Key verschlüsselt und kann in dieser Form im Benchmark Portal hochgeladen werden. Bitte ändern Sie den Dateinamen der GPG-Datei nicht ab, da dieser für eine Prüffunktion verwendet wird. Eine GPG-Datei mit verändertem Dateinamen kann u. U. nicht im Benchmark Portal hochgeladen werden.

**Benchmark Portal:** <https://benchmarkportal.his.solventum.de>

## 4.2 § 136-/eQS-Daten aufbereiten

The screenshot shows the 'Crypto Wizard' window of the Solventum software. The interface is in German and guides the user through encrypting data. At the top, it says 'Bitte wählen Sie, welche Art von Datensatz Sie verschlüsseln möchten:' (Please select the type of dataset you want to encrypt). A dropdown menu is set to '§ 136 Daten (inkl. PID-Bereinigung)'. Below this, it says 'Bitte wählen Sie einen oder mehrere Ordner mit je einem zu verschlüsselnden Datensatz:' (Please select one or more folders, each containing a dataset to be encrypted). There is a text input field for this selection and a green button labeled '+ Durchsuchen...' (Search...). A checkbox labeled 'Ausgabe im Standard-Ausgabeordner' (Output in standard output folder) is checked. A large grey button labeled 'Bereinigen & Verschlüsseln' (Clean & Encrypt) is below the input field. A 'Hinweis:' (Note) section contains instructions: 'Sie können hier einen oder mehrere Ordner oder schon komprimierte Dateien (Endung .zip, .7z oder .rar) mit jeweils beliebig vielen § 136-Exportdateien im Inhalt auswählen.' (You can select one or more folders or already compressed files with various § 136 export files in the content here.) and 'Bitte je ausgewähltem Ordner bzw. je komprimierter Datei nur Exporte für maximal ein IK und ein Auswertungsjahr verwenden.' (Please use exports for a maximum of one institution code and one evaluation year per selected folder or compressed file.) It also recommends using all processes of a year plus the previous year's summary in one folder. At the bottom right, there is a button 'Zurück zum Hauptmenü' (Back to main menu).

Wählen Sie zunächst die Datensatzart „§ 136 Daten“ aus.

Um eine oder mehrere Datei(en) auszuwählen, klicken Sie bitte auf

+ Durchsuchen...

Im folgenden Dialog wählen Sie bitte **Ordner** mit eQS-Daten aus. Mehrere Ordner können durch Halten der Strg-Taste und Anklicken einzelner Ordner ausgewählt werden. Alternativ können hier auch ZIP-Archivdateien ausgewählt werden. **Bitte achten Sie darauf, dass pro gewähltem Ordner bzw. komprimierter Datei nur Exporte für maximal ein Institutionskennzeichen (IK) und ein Auswertungsjahr enthalten sein dürfen.**

**Außerdem empfehlen wir alle relevanten Exportdateien mit allen Vorgängen eines Jahres + Überlieger aus dem Vorjahr mit gemeinsamem IK in einem Ordner abzulegen (ggf. in Unterordnern) und diesen auszuwählen. Dann erhalten Sie eine einzige verschlüsselte Datei pro Krankenhaus als Ergebnis und brauchen nur diese eine hochzuladen.**

Die Ausgabeordner werden dann im Normalfall am selben Ort abgelegt, an dem auch die Eingabeordner gespeichert sind. Alternativ können Sie die Option

☒ Ausgabe im Standard-Ausgabeordner


durch Setzen des Hakens aktivieren. Die Ausgabeordner werden dann im Ordner „Crypto Wizard Ausgabe“ in Ihrem persönlichen Dokumentenordner abgelegt. Wo genau dieser Ordner auf Ihrem System zu finden ist, wird Ihnen in einem Tooltip angezeigt. Halten Sie dazu den Mauszeiger etwas länger über die Checkbox.


Um die Aufbereitung der Daten zu starten, klicken Sie auf


Bereinigen & Verschlüsseln

Bitte beachten Sie, dass bei großen/vielen § 136-Dateien (oder mehreren gleichzeitig zur Verarbeitung ausgewählten Datensätzen) mit langen Laufzeiten zu rechnen ist. Befindet sich zudem der Speicherort der Eingabedaten und/oder der Ausgabedaten auf einem Netzlaufwerk, verlängert sich die Laufzeit entsprechend, da die Daten über das Netzwerk geladen werden müssen.

Nach Abschluss der Verarbeitung legt der Crypto Wizard im Zielordner einen Ausgabeordner (benannt mit „P136\_“, Institutionskennzeichen, Datenjahr, Name des gewählten Originalordners) mit folgendem Inhalt an:

 Bereinigt

 Original

 P136\_232323232\_2024\_2692662012434971.zip.gpg

Im Ordner „Bereinigt“ wird eine komprimierte ZIP-Datei abgelegt, in der sich die reduzierten bzw. bereinigten Datensätze (Original ohne PID-Infos) befinden.

Im Ordner „Original“ befinden sich die Original- bzw. unbehandelten Daten als komprimiertes ZIP-Archiv.

Neben diesen beiden Ordnern finden Sie auch die fertig verschlüsselte GPG-Datei (benannt mit „P136\_“, Institutionskennzeichen, Datenjahr und einem Zahlencode). Diese Datei, welche die bereinigten eQS-Daten enthält, ist mit dem Solventum-Datenservice-Key verschlüsselt und kann in dieser Form im Benchmark Portal hochgeladen werden.

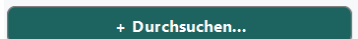
Bitte ändern Sie den Dateinamen der ZIP.GPG-Datei nicht ab, da dieser für eine Prüffunktion verwendet wird. Eine GPG-Datei mit verändertem Dateinamen kann u. U. nicht im Benchmark Portal hochgeladen werden.

### 4.3 SpiGes-Daten aufbereiten

Wählen Sie zunächst die Datensatzart „SpiGes Daten“ aus.

**Bitte achten Sie bei SpiGes-Daten unbedingt darauf, dass die enthaltenen Fall\_id's **nicht** bereits zuvor eine andere Pseudonymisierungsfunktion durchlaufen haben.**

Um einen oder mehrere Datensatz/Datensätze auszuwählen, klicken Sie bitte auf



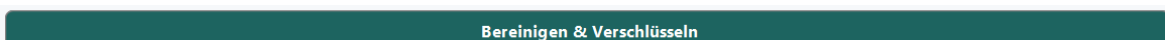
Im folgenden Dialog wählen Sie bitte **Ordner**, mit je einem Datensatz aus (beinhaltet jeweils nur eine SpiGes XML Datendatei). Mehrere Ordner können durch Halten der Strg-Taste und Anklicken einzelner Ordner ausgewählt werden. Alternativ können hier auch ZIP-Archivdateien ausgewählt werden, die jeweils einen SpiGes-Datensatz enthalten müssen. **Bitte achten Sie darauf, dass jeder SpiGes-Datensatz jeweils nur Daten einer Spital-ID und eines Datenjahres enthält. Die Daten mehrerer Standorte pro Datensatz sind jedoch möglich.**

Die Ausgabeordner werden dann im Normalfall am selben Ort abgelegt, an dem auch die Eingabeordner gespeichert sind. Alternativ können Sie die Option



durch Setzen des Hakens aktivieren. Die Ausgabeordner werden dann im Ordner „Crypto Wizard Ausgabe“ in Ihrem persönlichen Dokumentenordner abgelegt. Wo genau dieser Ordner auf Ihrem System zu finden ist, wird Ihnen in einem Tooltip angezeigt. Halten Sie dazu den Mauszeiger etwas länger über die Checkbox.





Um die Aufbereitung der Daten zu starten, klicken Sie auf



Bitte beachten Sie, dass bei sehr großen SpiGes-Datensätzen (oder mehreren gleichzeitig zur Verarbeitung ausgewählten Datensätzen) mit langen Laufzeiten zu rechnen ist, da zahlreiche Änderungen in einer sehr großen XML-Struktur vorgenommen werden müssen. Befindet sich zudem der Speicherort der Eingabedaten und/oder der Ausgabedaten auf einem Netzlaufwerk, verlängert sich die Laufzeit entsprechend, da die Daten über das Netzwerk geladen werden müssen.

**Richtwert: 5 Minuten Laufzeit / 20.000 Fälle.**

Nach Abschluss der Verarbeitung legt der Crypto Wizard im Zielordner pro Datensatz je einen Ausgabeordner (benannt mit „SpiGes\_“, Spital\_ID, Datenjahr, Name des gewählten Originalordners) und folgendem Inhalt an:

-  Bereinigt
-  Mappingdatei
-  Original
-  SpiGes\_12345678\_2024\_326518200332305633300191.zip.gpg

Im Ordner „Mappingdatei“ finden Sie die Mappingdatei (benannt mit „Mappingdatei\_“, Spital\_ID, Datenjahr, Erstellungsdatum und Uhrzeit).

Über diese Datei kann ein direkter Bezug zwischen der Original-Fall\_id und dem im Datensatz eingesetzten Pseudonym hergestellt werden. **Bitte senden Sie diese Datei niemals an Solventum.** Sie benötigen diese Datei später, um in fallbezogenen Ergebnissen, die Sie von Solventum erhalten, einen Bezug zur Original-Fallnummer herstellen zu können. **Bitte bewahren Sie diese Datei daher an einem sicheren Speicherort auf.**

Im Ordner „Original“ finden Sie den Original-Datensatz als ZIP-Archiv. Über diese Datei können Sie zu einem späteren Zeitpunkt genau nachvollziehen, welche Datengrundlage für die Datenaufbereitung verwendet wurde.

Im Ordner „Pseudonymisiert“ finden Sie den erzeugten Datensatz (pseudonymisiert und reduziert) als ZIP-Archiv. Über diese Datei können Sie das Ergebnis der Datenaufbereitung nachvollziehen.

Neben diesen drei Ordnern finden Sie auch die fertig verschlüsselte GPG-Datei (benannt mit „SpiGes\_“, Spital\_ID, Datenjahr und einem Zahlencode).

Diese Datei, welche den pseudonymisierten Datensatz enthält, ist mit dem Solventum-Datenservice-Key verschlüsselt und kann in dieser Form im Benchmark Portal hochgeladen werden. Bitte ändern Sie den Dateinamen der GPG-Datei nicht ab, da dieser für eine Prüffunktion verwendet wird. Eine GPG-Datei mit verändertem Dateinamen kann u. U. nicht im Benchmark Portal hochgeladen werden.

**Benchmark Portal:** <https://benchmarkportal.his.solventum.de>

## 4.4 Andere Datensätze aufbereiten

Wählen Sie die Datensatzart „Andere Datensatzformate“ aus.

Unter „Andere Datensatzformate“ fallen alle Daten, die nicht zu den § 21-, § 136- oder SpiGes-Daten gehören (z. B. spezielle Formate). Falls Sie sich nicht sicher sind, welche Funktion für Ihre Datenübermittlung die Richtige ist, dann rufen Sie uns bitte an. Wir unterstützen Sie gerne bei der Verschlüsselung.

Um einen oder mehrere Datensätze bzw. Datenlieferungen zur Verschlüsselung auszuwählen, klicken Sie bitte auf .

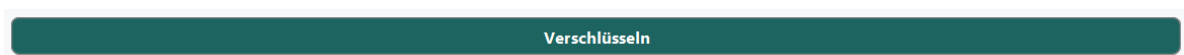
Im folgenden Dialog wählen Sie bitte alle Dateien aus, die zu je einer separaten Lieferung verschlüsselt werden sollen (mehrere Dateien können durch Halten der Strg-Taste und Anklicken einzelner Dateien ausgewählt werden). Die Dateien müssen alle im selben Ordner gespeichert sein, sonst ist die Mehrfachauswahl nicht möglich.

Bestehen die zu verschlüsselnden Datensätze bzw. Datenlieferungen jeweils aus mehr als einer Datei, so müssen diese vorab zu einer ZIP-Archivdatei zusammengefasst werden, um am Ende des Verschlüsselungsprozesses nur eine GPG-Datei je Datensatz bzw. Datenlieferung zu erhalten.

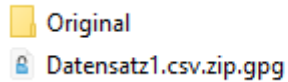
Die Ausgabeordner werden am selben Ort abgelegt, an dem auch die Eingabedateien gespeichert sind. Alternativ können Sie die Option

durch Setzen des Hakens aktivieren. Die Ausgabeordner werden dann im Ordner „Crypto Wizard Ausgabe“ in Ihrem persönlichen Dokumentenordner abgelegt. Wo genau dieser Ordner auf Ihrem System zu finden ist, wird Ihnen in einem Tooltip angezeigt. Halten Sie dazu den Mauszeiger etwas länger über die Checkbox.

Um die Verschlüsselung der Daten zu starten, klicken Sie auf



Nach Abschluss der Verschlüsselung legt der Crypto Wizard im Zielordner einen Ausgabeordner (benannt mit dem Namen und der Dateiendung der Eingabedatei) und folgendem Inhalt an:



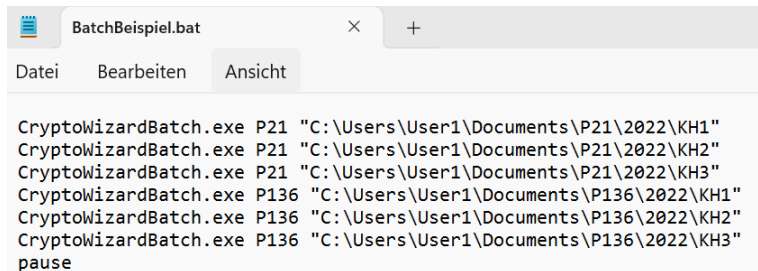
Im Ordner „Original“ finden Sie den Original-Datensatz als ZIP-Archiv. Über diese Datei können Sie zu einem späteren Zeitpunkt genau nachvollziehen, welche Datengrundlage für die Verschlüsselung verwendet wurde.

Daneben finden Sie im Ausgabeordner auch die fertig verschlüsselte GPG-Datei (benannt wie die Eingabedatei mit den zusätzlichen Dateiendungen „.zip.gpg“). Diese Datei ist mit dem Solventum-Datenservice-Key verschlüsselt und kann in dieser Form im Benchmark Portal hochgeladen werden.

**Benchmark Portal:** <https://benchmarkportal.his.solventum.de>

## 4.5 Batch-Modus

Benutzer, die Datensätze vieler Kliniken für die Lieferung an Solventum verschlüsseln möchten, können dafür, neben der Auswahl mehrerer Ordner zur Verschlüsselung über die Benutzeroberfläche, auch den Batch-Modus nutzen. Hierzu muss vorab eine Batch-Datei gepflegt werden. Ein Beispiel für den Aufbau der Batch-Datei finden Sie in der Abbildung. Die Datei „BatchBeispiel.bat“ wird auch im Crypto Wizard Programmordner mitgeliefert.



```

CryptoWizardBatch.exe P21 "C:\Users\User1\Documents\P21\2022\KH1"
CryptoWizardBatch.exe P21 "C:\Users\User1\Documents\P21\2022\KH2"
CryptoWizardBatch.exe P21 "C:\Users\User1\Documents\P21\2022\KH3"
CryptoWizardBatch.exe P136 "C:\Users\User1\Documents\P136\2022\KH1"
CryptoWizardBatch.exe P136 "C:\Users\User1\Documents\P136\2022\KH2"
CryptoWizardBatch.exe P136 "C:\Users\User1\Documents\P136\2022\KH3"
pause
  
```

Es müssen zwei Parameter an die „CryptoWizardBatch.exe“ übergeben werden:

1. Typ des zu verschlüsselnden Datensatzes: [P21|P136]
2. Ordner (vollständiger Pfad) in dem der zu verschlüsselnde Datensatz gespeichert ist. Dieser sollte in Anführungszeichen gesetzt werden, wenn Leerzeichen im Pfad enthalten sind.

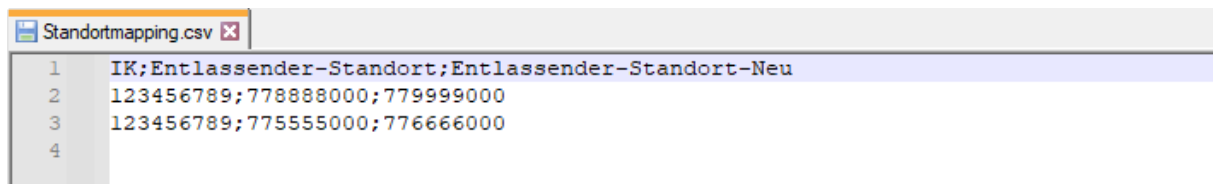
Der Ausgabeordner wird, entsprechend dem Standard-Verfahren bei der Verschlüsselung über die Benutzeroberfläche, im selben Ordner gespeichert wie der Eingabeordner.

## 4.6 Standortmapping

Für die Verarbeitung von Daten nach § 21 oder § 136 wurde eine Standortmapping-Funktion implementiert. Diese ermöglicht die Ersetzung von Standortkennzeichen im gesamten Datensatz, sowie in der bei der § 21-Pseudonymisierung erzeugten Fallnummern-Mappingdatei.

Diese Funktionalität wird i.d.R. nach entsprechender Vereinbarung mit dem Solventum Datenservice genutzt. Möglicherweise erhalten Sie dazu eine speziell auf Ihre Daten vorbereitete Mappingdatei. Nutzen Sie bitte nur diese für das Standortmapping, da es sonst zur Zuordnung Ihrer Daten zu falschen Standorten kommen kann.

Die Mappingdatei „Standortmapping.csv“ wird vom Crypto Wizard automatisch verwendet, sobald sie sich im Konfigurationsordner „Crypto Wizard Konfiguration“ in Ihrem persönlichen Dokumentenordner (i. d. R. „Eigene Dateien“ bzw. „Dokumente“) befindet.



```

1 IK;Entlassender-Standort;Entlassender-Standort-Neu
2 123456789;778888000;779999000
3 123456789;775555000;776666000
4
  
```

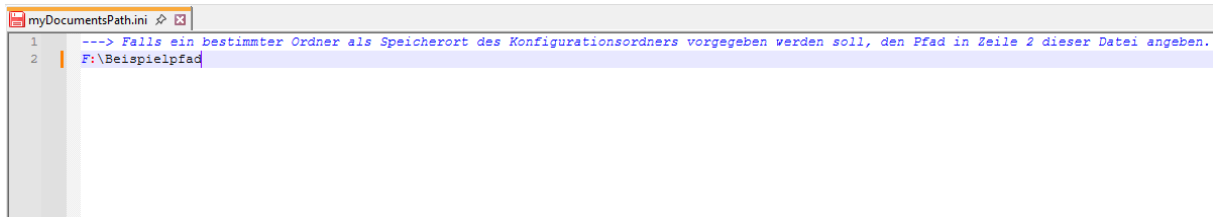
Falls nutzbare Einträge zum Mapping Ihrer Standorte gefunden werden, zeigt der Crypto Wizard dies während der Verarbeitung Ihrer Daten an bzw. gibt entsprechende Informationen in der Logdatei aus.



#### 4.7 Konfigurationsordner anpassen

In manchen Konfigurationen sind die benutzerabhängigen Dokumentenordner (i. d. R. „Eigene Dateien“ bzw. „Dokumente“) im Windows-System nicht definiert oder nicht bzw. nicht praktikabel als Ort für den Konfigurationsordner „Crypto Wizard Konfiguration“ nutzbar. Für solche Fälle kann der Pfad zum Konfigurationsordner, den der Crypto Wizard verwenden soll angepasst werden.

Dazu muss in der Datei „myDocumentsPath.ini“ der gewünschte Pfad in der 2. Zeile hinterlegt werden:

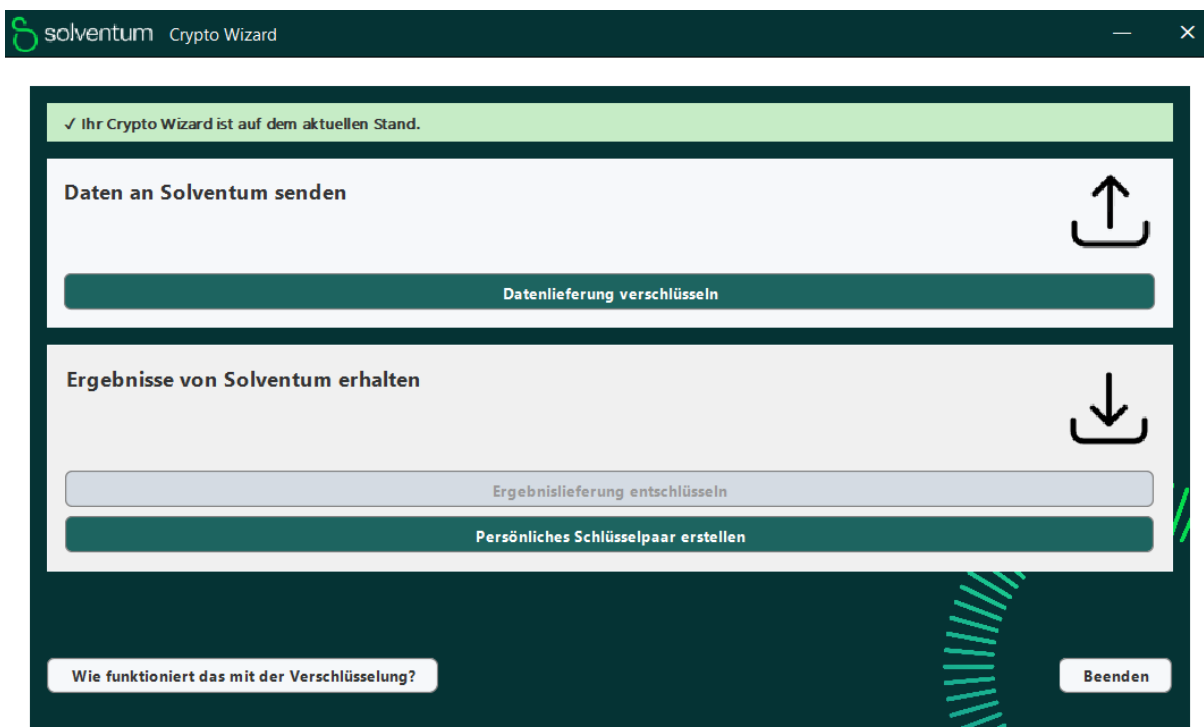


```
1  ---> Falls ein bestimmter Ordner als Speicherort des Konfigurationsordners vorgegeben werden soll, den Pfad in Zeile 2 dieser Datei angeben.
2  F:\Beispielpfad
```

Diese Datei finden Sie bereits vorbereitet im Unterordner „config“ im Crypto Wizard-Programmordner.

## 5. Ergebnisse von Solventum erhalten

Unter diesem Punkt können Sie die Ergebnislieferungen entschlüsseln. Im Vorfeld ist es erforderlich, Ihr eigenes asymmetrischen GPG-Schlüsselpaar zu erstellen. Der öffentliche Schlüssel wird, wie weiter unten beschrieben, im Benchmark Portal hochgeladen.



Beim ersten Start des Crypto Wizard erscheint der Punkt „Ergebnislieferung entschlüsseln“ deaktiviert, da Sie für die Nutzung dieser Funktion erst ein persönliches Schlüsselpaar erstellen und den öffentlichen Teil im Benchmark Portal hochladen müssen.

**ACHTUNG! Solange der Crypto Wizard die Entschlüsselung von Dateien durchführt, ist eine erneute Erstellung eines Schlüsselpaars nicht erforderlich.**

### 5.1 Persönliches Schlüsselpaar erstellen

Um das Schlüsselpaar zu erzeugen, klicken Sie bitte auf



Im folgenden Fenster tragen Sie bitte Ihren Namen, den Namen Ihres Krankenhauses oder Trägers sowie Ihre E-Mail-Adresse ein.

**solventum** Crypto Wizard

**Erforderliche Angaben:**

Ihr Name

Krankenhaus / Träger

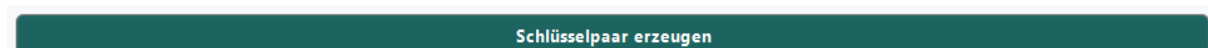
E-Mail-Adresse

Bitte beachten Sie, dass Sie nur den öffentlichen Schlüssel mit der Dateiendung ".pub" an Dritte weitergeben, in diesem Fall dem Solventum Datenservice. Die Datei mit der Endung ".sec" ist Ihr privater Schlüssel, welcher ausschließlich Sie dazu befähigt, die für Sie bereit gestellten Ergebnisse zu entschlüsseln.

Schlüsselpaar neu erzeugen

Zurück zum Hauptmenü

Bestätigen Sie bitte die folgende Schaltfläche, um das Schlüsselpaar zu erzeugen.



Bitte beachten Sie, dass Sie nur den öffentlichen Schlüssel mit der Dateiendung ".pub" an andere Personen, in diesem Falle an den Solventum Datenservice, weitergeben. Die Datei mit der Endung ".sec" ist Ihr privater Schlüssel, welcher ausschließlich Sie dazu befähigt, die für Sie bereit gestellten Ergebnisse zu entschlüsseln.

Nach Erzeugen des Schlüssels wird der Hinweistext durch den in der folgenden Abbildung aufgeführten Hinweis ersetzt. Es wird der Name des Schlüssels angezeigt sowie am unteren Rand des Fensters der Ordnerpfad, in dem Ihr persönliches Schlüsselpaar gespeichert wird. Der Ordner (benannt „Crypto Wizard Konfiguration“) wurde vom Crypto Wizard in Ihrem persönlichen Dokumentenordner erstellt (i. d. R. „Eigene Dateien“ bzw. „Dokumente“).

**ACHTUNG! Verschieben oder löschen Sie bitte keinesfalls die Inhalte dieses Ordners, da der Crypto Wizard bei jedem Entschlüsseln einer Datei auf den privaten Schlüssel zugreifen muss.**

**solventum Crypto Wizard**

Erforderliche Angaben:

Ihr Name

Krankenhaus / Träger

E-Mail-Adresse

Das Schlüsselpaar wurde erfolgreich generiert. Der öffentliche Schlüssel **Schlüsselname** wurde zusätzlich auf dem Desktop abgelegt. Bitte laden Sie diesen im Solventum Benchmark Portal hoch. Melden Sie sich dort mit Ihrem Benutzernamen und Passwort an. Klicken Sie dann in der Menüleiste auf "Ihr Profil" und dann auf "Ihr öffentlicher Schlüssel".

Konfigurationsordner: C:\ **Ordnerpfad** \Dokumente\Crypto Wizard Konfiguration 2026.1.0

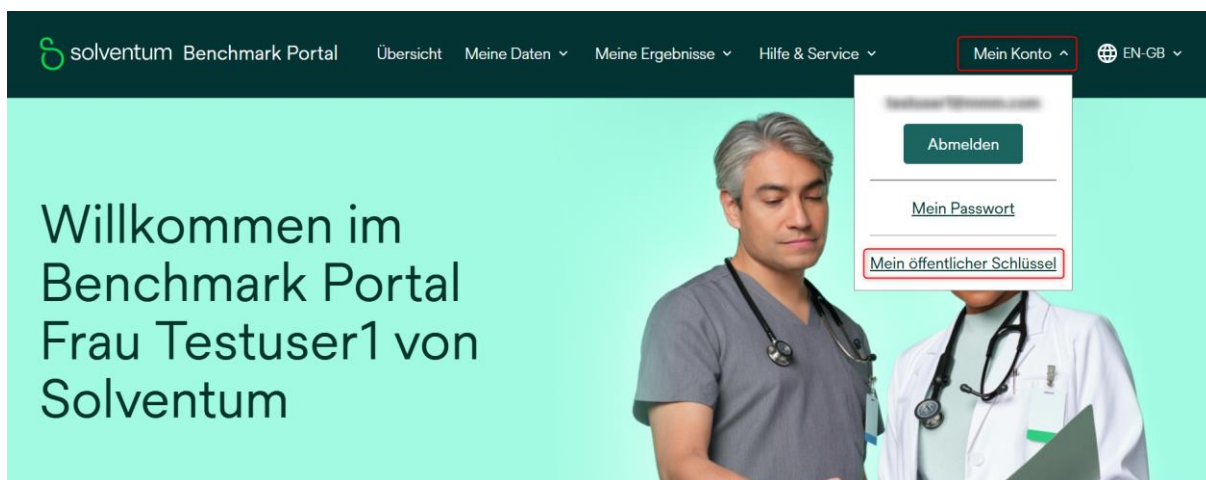
Eine Kopie des öffentlichen Schlüssels wird zusätzlich auf Ihrem Windows-Desktop abgelegt. Bitte laden Sie diesen, wie im Folgenden beschrieben, im Benchmark Portal hoch.

Um das Fenster zu verlassen, klicken Sie .

## 5.2 Hochladen des öffentlichen Schlüssels

**Benchmark Portal:** <https://benchmarkportal.his.solventum.de>

Melden Sie sich dort mit Ihrem Benutzernamen und Passwort an. Klicken Sie dann in der Menüleiste auf "Mein Konto" und dann auf "Mein öffentlicher Schlüssel".



Nicht mehr aktuell? Dann hier neuen öffentlichen Schlüssel hochladen:

Dateiauswahl

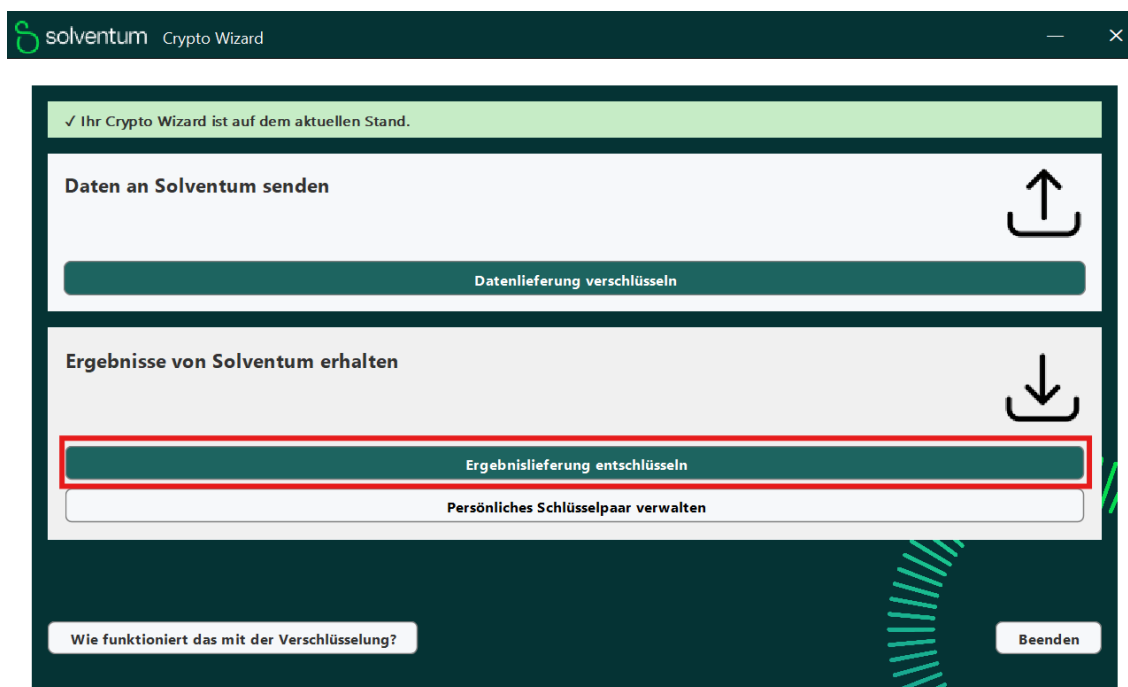
PUB-Datei in das Feld ziehen oder hier klicken für Dateiauswahl

Ausgewählte Schlüsseldatei hochladen

Bitte klicken Sie zum Hochladen des öffentlichen Schlüssels in das Feld „Dateiauswahl“ oder ziehen Sie den Schlüssel mit der Endung „.pub“ per Drag&Drop in das Feld. Klicken Sie anschließend auf „Ausgewählte Schlüsseldatei hochladen“.

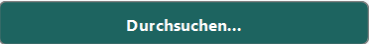
### 5.3 Ergebnislieferung des Solventum Datenservice entschlüsseln

Unter diesem Punkt können Sie die Ergebnislieferung entschlüsseln, die von Solventum mit Ihrem öffentlichen Schlüssel verschlüsselt wurde. D. h., dies ist erst dann möglich, wenn Sie ein persönliches Schlüsselpaar erstellt, den öffentlichen Teil im Benchmark Portal hochgeladen und danach ein verschlüsseltes Download-Paket mit Auswertungsergebnissen angefordert haben.




Um von Solventum erhaltene Dateien zu entschlüsseln, klicken Sie auf „Ergebnislieferung entschlüsseln“.

Sollte die o. g. Schaltfläche inaktiv sein, dann wurde innerhalb Ihres Windows-Kontos noch kein persönliches Schlüsselpaar erzeugt. Lesen Sie dazu im Kapitel [„Persönliches Schlüsselpaar erstellen“](#) weiter.

Um eine oder mehrere Dateien zu wählen, klicken Sie bitte auf  und wählen Sie bitte die Datei(en) aus, die Sie von Solventum erhalten haben. Diese ist üblicherweise an der Dateiendung ".gpg" erkennbar (mehrere Dateien können durch Halten der Strg-Taste und anklicken jeder einzelnen Datei ausgewählt werden).

Klicken Sie anschließend auf

Die entschlüsselte(n) Datei(en) wird/werden dann im Quellordner abgelegt.

Ist die Option  Archiv(e) nach der Entschlüsselung dekomprimieren aktiviert, werden die bei der Entschlüsselung entstandenen ZIP-Archivdateien im Anschluss entpackt, damit Sie direkt auf die Inhalte zugreifen können.

## Anhang

### Verschlüsselungsverfahren

Mit dem Crypto Wizard haben wir die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umgesetzt.

Wir nutzen eine hybride Verschlüsselung nach dem OpenPGP-Standard unter Verwendung der Software „GNU Privacy Guard“ (GnuPG):

1. Nachrichtenverschlüsselung mit symmetrischem Algorithmus AES-256
2. Session-Key-Verschlüsselung unter Verwendung asymmetrischer Algorithmen:
  - a. Übertragung zu Solventum → asymmetrische Verschlüsselung mit 2048 Bit RSA-Schlüssel
  - b. Übertragung zum Nutzer → asymmetrische Verschlüsselung mit 4096 Bit RSA-Schlüssel

### Weitere Lizenzbedingungen

Die Ver- und Entschlüsselung erfolgt unter Verwendung der Software „GNU Privacy Guard“ (GnuPG) von der Free Software Foundation Inc., welche unter der GNU GENERAL PUBLIC LICENSE steht.



**Solventum Germany GmbH**  
Health Information Systems

Standort Düsseldorf  
Kesselstraße 3 / 40221 Düsseldorf  
Telefon: 0211 / 7374 1234  
E-Mail: [datenservice@solventum.com](mailto:datenservice@solventum.com)

Please recycle. Printed in Germany  
All rights reserved