AUDIT-RAHMENWERK ZUM PSEUDONYMISIEREN VON VIACRYP B.V. 2017

VIACRYP B.V. Danzigerkade 19, NL-1013 AP Amsterdam

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument stellt das Audit-Rahmenwerk von Viacryp dar. Mit der Durchführung von Audits auf Grundlage dieses Rahmenwerks verfolgt die Firma Viacryp das Ziel, ihre Rolle als unabhängige Trusted Third Party zu bestätigen und den Nachweis zu erbringen, dass sie personen- und verhaltensbezogene Daten auf sichere und kontrollierte Weise verarbeitet.

1.1. Hintergründe

1.1.1. Pseudonymisieren

Unter „Pseudonymisieren" wird die Umwandlung personenbezogener Daten in einen nicht der ursprünglichen Person zuzuordnenden, eindeutigen Code verstanden. Pseudonymisieren ist ein wiederholbarer Prozess in dessen Rahmen die unmittelbar personenbezogenen Daten innerhalb einer vereinbarten Frist zu einem eindeutigen Pseudonym führen. Dadurch ist es möglich ohne die Rückführbarkeit der personenbezogenen Daten:

- pseudonymisierte Daten aus unterschiedlichen Quellen zusammenzuführen
- pseudonymisierte Daten zu einem späteren Zeitpunkt mit neuen Daten anzureichern

Obwohl Pseudonyme gemäß dem (Datenschutz-)Gesetz[1] immer noch als personenbezogene Daten zu betrachten sind, gilt, dass mit Pseudonymen mehr Verarbeitungen möglich werden als mit nicht pseudonymisierten personenbezogenen Daten[2].

- Erwägungsgrund 26 des niederländischen Datenschutzgesetzes AVG lautet, dass Pseudonyme nicht als anonyme Daten betrachtet werden dürfen: „Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden."
- Dagegen wird in Erwägungsgrund 28 der Verordnung mitgeteilt: „Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken."

1.1.2. Dienste zum Schutz der Privatsphäre

Auch wenn auf Seiten des Auftraggebers eine ausreichende Rechtsgrundlage für die Verarbeitung vorliegt, können Dienste von Viacryp zum Schutz der Privatsphäre eingesetzt werden. Ein Beispiel für einen solchen Dienst ist der Filterdienst.

1.1.3. Pseudonymisierungsstraße

In der angebotenen Lösung von Viacryp findet die Pseudonymisierung innerhalb einer sog. Pseudonymisierungsstraße statt. Das Konzept der Pseudonymisierungsstraße besteht darin, dass niemand innerhalb dieser Straße über die personen- oder verhaltensbezogenen Daten, eine Kombination beider oder über eine Kombination der Daten, mit denen sich zusammen mit anderen Daten ein Bezug zwischen personenbezogenen Daten und Verhalten herstellen lässt, verfügt. Die ursprünglichen personen- und verhaltensbezogenen Daten sind ausschließlich bei der Quelle bekannt und lesbar.

[1] Am 25.Mai 2018 tritt die europäische Datenschutz-Grundverordnung (DSGV) in Kraft und damit erlischt das heutige niederländische Gesetz zum Schutz personenbezogener Daten Wet Bescherming Persoonsgegevens (WBP).
[2] Die niederländische Aufsichtsbehörde für den Datenschutz Autoriteit Persoonsgegevens (AP) hat mitgeteilt, ebenfalls diesen Standpunkt während der Zeit, in der das WBP noch gilt, zu vertreten.

INPUT

Name	E. Gabler
Geburtsdatum	12-08-1964
Geschlecht	F
Postleitzahl	10785
Hausnummer	17
Ländercode	DE
Ausweisnummer	T22000129

OUTPUT

Name	
Geburtsjahr	1964
Geschlecht	F
Postleitzahlengebiet	10785
Hausnummer	
Ländercode	DE
Ausweisnummer	
Pseudonym (Name)	DS2N56HDM0BF
Pseudonym (Personalien)	DS2BHJKQWE32
Pseudonym (Ausweisnummer)	DS2BU72RE#XSL

Jede Straße umfasst eine oder mehrere Quellen (Anbieter) personenbezogener Daten und einen Abnehmer der pseudonymisierten Ergebnisse. Jede Viacrypstraße besteht aus drei aufeinander abgestimmten Komponenten. Pseudonyme bestehen ausschließlich innerhalb einer spezifischen Straße. Daten können nicht über Straßen hinweg miteinander kombiniert werden. Innerhalb einer Verarbeitungsstraße wird eine personenbezogene Angabe immer zum selben Pseudonym führen.

Viacryp liefert sowohl den Anbietern wie auch den Abnehmern im Vorfeld konfigurierte Software, die den Pseudonymisierungsprozess unterstützt. Für die Anbieter handelt es sich dabei um das „Supply-"Modul. Bei Viacryp ist Software (Pseudonymizer) vorhanden mit der die personenbezogenen Daten in ein Pseudonym umgewandelt werden. Der Abnehmer kann anschließend auf Grundlage von Pseudonymen Daten aus verschiedenen Quellen zusammenführen und analysieren, ohne dass es dafür personenbezogener Daten bedarf.

Die Funktionsweise des Pseudonymisierungsprozesses wurde in dem Dokument „Faktenblatt Viacryp" veröffentlicht.

1.2. Viacryp

Viacryp bietet Dienste zur sicheren und kontrollierten Verarbeitung personenbezogener Daten in Pseudonyme an. Damit werden Kunden in die Lage versetzt, konform den für sie geltenden (Datenschutz-)Verordnungen Personenprofile aufzustellen und Verhalten zu analysieren.

Viacryp bietet Dienste für die nachträgliche Datenverarbeitung wie auch für die Echtzeit-Verarbeitung an. Außerdem berät und unterstützt die Firma Viacryp ihre Kunden beim Ergreifen angemessener Maßnahmen, um die Verarbeitung personenbezogener Daten sicher und gemäß den geltenden (Datenschutz-)Verordnungen derart durchzuführen, dass die Privatsphäre der betroffenen Personen auf bestmögliche Weise geschützt wird. Es unterliegt jedoch weiterhin der Verantwortung des Kunden konform den geltenden Gesetzen und Verordnungen vorzugehen.

Als Trusted Third Party (TTP) engagiert sich Viacryp als Vermittler zwischen dem oder den Lieferanten der originalen personenbezogenen Daten und dem Abnehmer der pseudonymisierten Daten. In dieser Rolle gewährleistet Viacryp, dass:

- Viacryp personenbezogene Daten immer gemäß den geltenden (Datenschutz-)Gesetzen verarbeitet
- Viacryp eine fachkundige Verschlüsselung der personenbezogenen Daten anwendet
- Viacryp für eine sorgfältige Schlüsselverwaltung zur optimalen Geheimhaltung der Daten Sorge trägt
- Viacryp eine unabhängige, interessenneutrale Position einnehmen kann, da Viacryp keinen Zugang zu einer lesbaren Form der zu verarbeitenden oder verarbeiteten personenbezogenen oder anderen Daten hat

1.3. Zweck dieses Dokuments

Dieses Dokument ist der Leitfaden für das Audit der Dienste von Viacryp. Das Audit hat die Erbringung des Nachweises zum Ziel, dass Viacryp in der Lage ist, auf sichere und kontrollierte Weise personenbezogene Daten zu pseudonymisieren. Das Audit bezieht sich auf die technischen und internen, organisatorischen Maßnahmen sowie die Verantwortungsbereiche, die durch ihr Zusammenwirken die sichere und kontrollierte Verarbeitung personenbezogener Daten gewährleisten.

Viacryp hat Technologien entwickelt und Prozesse zur Pseudonymisierung personenbezogener Daten eingerichtet, wodurch die Umkehrung der Verschlüsselung („Replay Attack“) erheblich erschwert wird[3]. Ihre unabhängige und interessenneutrale Position als TTP gewährleistet Viacryp durch technische und organisatorische Maßnahmen, die die Einsichtnahme in die Daten in lesbarer Form während des Verarbeitungsprozesses ausschließt. Viacryp stellt sich selbst die folgenden Kriterien, um nachzuweisen, dazu in der Lage zu sein:

- Die Pseudonymisierung wird auf fachkundige Weise eingesetzt und dabei findet die erste Verschlüsselung beim Anbieter der Daten statt.
- Es wurden technische und organisatorische Maßnahmen ergriffen, um die Umkehrung der Verschlüsslung („Replay Attack“) zu verhindern und zu verhindern, dass Viacryp einen Einblick in oder Zugriff auf für Menschen lesbare Daten erhält.
- Um jeden Betroffenen in die Lage zu versetzen, sich über die gebotenen Garantien informieren zu können, wurde die eingesetzte Pseudonymisierungslösung in einem öffentlich verfügbaren Dokument dargestellt.

1.4. Gliederung des Dokuments

In Kapitel 2 werden die Hintergründe und die Untersuchungsarten dargestellt, die durchgeführt werden, um nachzuweisen, dass den Kriterien, wie in Paragraf 1.3 aufgeführt, entsprochen wird. In Kapitel 3 werden die durchzuführenden Untersuchungen dargestellt, die den Nachweis zu erbringen haben, dass den gestellten Kriterien im Prozess entsprochen wird. Diese Untersuchungen richten sich nacheinander auf die Qualität und Sicherheit der eingesetzten Technik und die organisatorischen Maßnahmen, die Kundenvereinbarungen, die getroffen wurden und die Art und Weise, wie Viacryp ihre Kunden bei der Nutzung der Möglichkeit mit vollständig anonymen Daten zu arbeiten, unterstützt. In Kapitel 4 werden der Aufbau und die Durchführung des Auditprozesses dargestellt.

0 besteht aus einer Liste mit Abkürzungen und Definitionen, wie sie in diesem Dokument verwendet werden. 0 umfasst eine Übersicht der einzusetzenden Kontrollen und 0 bietet eine Übersicht etwaiger Defizite je Kriterium. 0 enthält eine Übersicht der eingesetzten Verschlüsselungstechniken.

[3] Vollständiger Schutz vor Replay Attacks ist ausschließlich möglich, wenn der Kunde selbst die entsprechenden Verfahrensmaßnahmen ergreift.

2. Untersuchungsarten

Um beurteilen zu können, ob Viacryp den in Paragraf 1.3 aufgeführten Kriterien entspricht, sind die folgenden Untersuchungen vorgesehen.

- 1. Untersuchung: Der funktionale Prozess und die technische Einrichtung der Technologie von Viacryp
  Eine Untersuchung nach der funktionalen und technischen Einrichtung der entwickelten Technologie, in deren Rahmen festgestellt wird, ob die Technologie die sichere, nicht lesbare und nicht umkehrbare Verarbeitung der Daten ausreichend gewährleistet.
- 2. Untersuchung: Management von Viacryp
  Diese Untersuchung bezieht sich auf die Managementumgebung, in der die Technologie von Viacryp untergebracht ist. Dabei werden die vom Management ergriffenen technischen und organisatorischen Maßnahmen überprüft.
- 3. Untersuchung: Kundenvereinbarungen
  In dieser Untersuchung werden die Kundenvereinbarungen überprüft, die zwischen Viacryp und ihren Kunden getroffen wurden.

Der Untersuchungsgegenstand besteht aus der verwirklichten Technologie, der ergriffenen Managementmaßnahmen in Bezug auf die kryptografischen Systeme und der (Management-)Prozesse für die generische Pseudonymisierung personenbezogener Daten.

Die Untersuchungen werden im nächsten Kapitel ausgearbeitet. Die anzuwendenden Kontrollen für das Audit-Rahmenwerk gemäß ISO 27001 und ISO 20000 sind in Anlage A.2 aufgeführt.

3. Untersuchungen

3.1. 1. Untersuchung: Der funktionale Prozess und die technische Einrichtung der Technologie von Viacryp

3.1.1. Zielsetzung

Die Zielsetzung besteht aus der Erbringung des Nachweises, dass die eingesetzten Technologien eine fachkundige und sichere Verarbeitung personen- und verhaltensbezogener Daten ausreichend gewährleisten. Konkret bedeutet das, dass die Technologie ausreichenden Schutz gegenüber Replay Attacks bietet und verhindert, dass personen- oder verhaltensbezogene Daten jeglicher Art innerhalb des Rahmens der Viacrypstraße lesbar oder einer Person zuzuordnen sind. Außerdem ist zu belegen, dass die öffentlich verfügbare Dokumentation mit der eingesetzten Technologie übereinstimmt.

3.1.2. Umfang

- Der Untersuchungsumfang umfasst folgende Aspekte:
  - Erste Verschlüsselung: Es wird erzwungen, dass die erste Verschlüsselung der personenbezogenen Daten am Standort der liefernden Partei stattfindet.
  - Unumkehrbar: Die erste Verschlüsselung der personenbezogenen Daten (der „Wer"-Teil) muss unumkehrbar sein, damit sich die personenbezogenen Daten an keiner Stelle im Laufe des weiteren Prozesses den ursprünglichen Werten zuordnen lassen.
  - Verschlüsselung des „Was"-Teils: die implementierte Technologie schließt aus, dass die nicht personenbezogenen Daten nach der Verschlüsselung wieder in lesbare Form umgewandelt werden können, abgesehen vom Zeitpunkt direkt nach dem Eingang beim Abnehmer.
  - Keys und Hashes generieren: die implementierte Technologie muss erzwingen, dass Hashes und Public/Private Keys ausschließlich von den dazu autorisierten Modulen generiert werden können.
  - Speicherung von Private Keys: die implementierte Technologie erzwingt eine sichere Speicherung der Private Keys.
  - State-of-the-Art Technologie: die eingesetzten Techniken und Algorithmen zur Verschlüsslung befinden sich durch die Nutzung von „Good Practices" und offenen Standards auf dem aktuellen Stand der Technik.

3.1.3. Durchführung

Im Rahmen dieser Untersuchung werden die folgenden Tätigkeiten durchgeführt:

- Beurteilung des funktionalen Pseudonymisierungsprozesses vom Supply- bis Delivery-Modul.
- Untersuchung der eingesetzten Viacryp-Software, des Supply-Moduls zur Beurteilung der folgenden Punkte:
  - Werden tatsächlich mehrere logische Kontrollen der angebotenen Daten durchgeführt?
  - Wird eine Spaltung zwischen den personenbezogenen Daten (der „Wer"-Teil) und den zugehörigen Daten (der „Was"-Teil) erzwungen? Damit die Daten an keiner Stelle in der Straße in lesbarer Form vorhanden sind, gemäß dem folgenden Schema:

	Quelle	Supply	Pseudonymizer	Delivery	Abnehmer
Wer	Original	Hashed & Verschlüsselt	Hashed	Pseudonym	Pseudonym
Was	Original	Verschlüsselt	Verschlüsselt	Verschlüsselt	Original

  - Wurde der „Wer"-Teil mithilfe einer Einweg Hashing-Technik gehasht?
  - Werden auf der Supply-Plattform der „Wer"-Teil und "Was"-Teil verschlüsselt bevor die Daten die Quelle verlassen?
  - Werden beide Teile mithilfe der Verschlüsselung derart geschützt, dass der „Wer"-Teil ausschließlich von Viacryp und der „Was"-Teil ausschließlich von der empfangenden Partei geöffnet werden kann?
  - Das Supply-Modul bietet Möglichkeiten, das Risiko der (unmittelbaren) Wiederherstellung des Personenbezugs der Daten zu verringern.
- Untersuchung zum Pseudonymizer innerhalb des Bereiches von Viacryp
  - Der Pseudonymizer überprüft die Authentizität der bereitgestellten Daten.
  - Der Pseudonymizer kann ausschließlich den bereitgestellten „Wer"-Teil entschlüsseln, um die gehashten Daten in Pseudonyme umzuwandeln.
- Untersuchung zum Delivery-Modul
  - Das Delivery-Modul überprüft die Authentizität der bereitgestellten Daten.
  - Auf der Delivery-Plattform werden die „Was"-Teile entschlüsselt und dem Abnehmer, gegebenenfalls mit den Pseudonymen, zur Verfügung gestellt.
- Untersuchung zur Verwaltung der Private Keys
  - Verfügen die betreffenden Module über ausreichende Möglichkeiten zur sicheren Speicherung der Private Keys?
- Untersuchung zur veröffentlichten Darstellung der Viacryp-Lösung:
  - Gibt es eine öffentlich verfügbare Dokumentation, in der die funktionale und technische Funktionsweise derart dargestellt wurden, dass die Betroffenen einen ausreichenden Einblick in die Art und Weise, wie personen- und verhaltensbezogene Daten verarbeitet werden, erhalten?
  - Wurde die untersuchte Viacryp-Lösung gemäß der öffentlich verfügbaren Dokumentation verwirklicht?
- Untersuchung zur State-of-the-Art Verschlüsselung
  - Findet eine regelmäßige und/oder systematische (interne oder externe) Überprüfung der eingesetzten Verschlüsselungstechnologie statt?
  - Werden die aktuellen Entwicklungen auf dem Gebiet der Verschlüsselungstechnologie und Informationssicherheit auf regelmäßige und/oder systematische Weise erfasst und in Konsequenzen für die eingesetzte Technologie umgesetzt?
- Untersuchung zu professionellen Entwicklungsmethoden
  - Findet die Softwareentwicklung konform einer bewährten Entwicklungsmethode statt, in der alle Phasen der Softwareentwicklung dargestellt werden?

3.2. 2. Untersuchung: Management von Viacryp

3.2.1. Zielsetzung

Die Zielsetzung besteht aus der Erbringung des Nachweises, dass technische und organisatorische Maßnahmen ergriffen wurden, die eine sichere Verarbeitung personen- und verhaltensbezogener Daten ausreichend gewährleisten. Konkret bedeutet das, dass die Technologie und die organisatorischen Maßnahmen ausreichenden Schutz gegenüber Replay Attacks bieten und verhindern, dass personen- oder verhaltensbezogene Daten jeglicher Art innerhalb der Viacrypstraße lesbar oder einer Person zuzuordnen sind. In dieser Untersuchung wird von der heutigen Situation des Hosting-Outsourcings und der Verwaltung der technischen Lösung bei einer Drittpartei (nachstehend „Hosting-Lieferant“ genannt) ausgegangen.

3.2.2. Umfang

Der Untersuchungsumfang umfasst folgende Punkte:

- Gestellte Anforderungen an die Managementprozesse: Untersuchung, ob die Vergabe und die Anforderungen, die Viacryp an den Hosting-Lieferanten stellt, ausreichende Sicherheiten für eine sichere Verarbeitung der Daten bieten. Es geht dabei um die Einrichtung der Prozesse zum Vorfalls-, Problem-, Änderungs- und Konfigurationsmanagement, gemäß ISO 20000-1 Paragraf 8.1 Vorfallsmanagement, 8.2 Problemmanagement, 9.1 Konfigurationsmanagement und 9.2 Veränderungsmanagement.
    - Informationssicherheit: Untersuchung, ob die Vergabe und die Anforderungen, die Viacryp an den Hosting-Lieferanten bezüglich der ergriffenen Sicherheitsmaßnahmen stellt, ausreichend sicherstellen, dass die Verschlüsselung angemessen bleibt. Als diesbezügliche Norm werden die ISO 27001:2013 / ISO 27002:2013 *Normen bzw. Praxisrichtlinien zur Informationssicherheit* eingesetzt. Eine Anwendbarkeitserklärung ist von Viacryp vorzulegen. Das Audit bezieht sich auf die Kontrollmaßnahmen in der Anwendbarkeitserklärung. Es geht dabei spezifisch um die Paragrafen A.9.1 (Geschäftsanforderungen an die Zugangssteuerung), A.10.1 (Kryptografische Maßnahmen), A13.2 (Informationsübertragung) und A.15.1 (Informationssicherheit in Lieferantenbeziehungen).
- Überprüfung durch Viacryp: Untersuchung, ob Viacryp in ausreichendem Maße überprüft hat, ob der Hosting-Lieferant die gestellten Anforderungen erfüllt hat.
    - Überwachung, Autorisierung, Entwicklung, Änderungs- und Releasemanagement, Datensicherung gemäß ISO 27001 / ISO 27002 Paragrafen: A.12 (Betriebssicherheit) und A.16.1 (Handhabung von Informationssicherheitsvorfällen und Verbesserungen)

3.3. 3. Untersuchung: Kundenvereinbarungen

3.3.1. Zielsetzung

Die Zielsetzung besteht aus der Erbringung des Nachweises, dass Viacryp mit Kunden angemessene, klare Vereinbarungen zu den durchzuführenden Tätigkeiten trifft. Diese Untersuchung soll außerdem belegen, dass Viacryp eine unabhängige Position einnimmt, wie es der Rolle einer Trusted Third Party entspricht.

3.3.2. Umfang

- Werden Kunden auf angemessene Weise auf Risiken und Verantwortlichkeiten hingewiesen, unter Berücksichtigung der Frage bis zu welchem Grad der Kunde selbst in der Lage ist, ein qualifiziertes Urteil bezüglich der Rechtmäßigkeit der durchzuführenden Verarbeitung abzugeben.
- Werden ausreichende Maßnahmen auf Grundlage von „Industry Good Practices“ und/oder Erfahrungen von Viacryp dargestellt?

3.3.3. Durchführung

In dieser Untersuchung werden die folgenden Tätigkeiten durchgeführt:

- Überprüfung der allgemeinen Bedingungen von Viacryp
- Überprüfung der Verträge mit den Kunden von Viacryp
- Überprüfung der gesetzlich vorgeschriebenen Dokumente, wie Vereinbarungen zur Auftragsdatenverarbeitung
- Überprüfung etwaiger schriftlicher Handlungsempfehlungen

4. Der Auditprozess

4.1. Einleitung

In diesem Kapitel wird dargestellt, wie die unabhängige Audituntersuchung zu verlaufen hat. Dabei wurden die NEN-EN-ISO 19011 Richtlinien zur Durchführung von Audits berücksichtigt. Ein Audit ist ein systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und deren objektiver Auswertung, um zu ermitteln, inwieweit die vereinbarten Auditkriterien erfüllt sind. Diese internationale Norm stellt keine Anforderungen, sondern erteilt Richtlinien für das Management eines Auditprogramms, das Planen und Durchführen eines Audits des Managementsystems und für die Kompetenz und Beurteilung eines Auditors und eines Auditteams.

4.2. Für die Durchführung eines Audits geltende Prinzipien

Die Durchführung eines Audits stützt sich auf eine Reihe von Prinzipien. Diese Prinzipien sollen dazu beitragen, dass es sich bei dem Audit um ein effektives und zuverlässiges Instrument zur Unterstützung von Management- und Kontrollmaßnahmen auf Seiten der Geschäftsleitung von Viacryp handelt, indem Informationen erbracht werden, auf deren Grundlage eine Organisation Maßnahmen zur Verbesserung ihrer Leistungen ergreifen kann. Die Beachtung dieser Grundsätze ist eine erste Voraussetzung für die Aufstellung von Auditschlussfolgerungen, die relevant und ausreichend sind und um Auditoren in die Lage zu versetzen, unabhängig voneinander zu arbeiten und zu vergleichbaren Schlussfolgerungen unter vergleichbaren Umständen zu gelangen.

4.2.1. Integrität

Integrität: die Grundlage des Berufsbildes. Auditoren und die Person, die ein Auditprogramm leitet, haben:

- ihre Arbeit auf ehrliche, sorgfältige und verantwortungsbewusste Weise durchzuführen
- sich an die geltenden gesetzlichen Anforderungen zu halten und ihnen Folge zu leisten
- bei der Durchführung ihrer Arbeit einen Nachweis ihrer Kompetenz zu erbringen
- ihre Arbeit auf unparteiliche Weise auszuführen, d.h. bei ihrem Vorgehen immer ehrlich und unvoreingenommen zu bleiben
- bedachtsam hinsichtlich aller Faktoren zu sein, die ihr Urteil bei der Durchführung eines Audits beeinflussen können

4.2.2. Sachliche Darstellung

Sachliche Darstellung besteht aus der Pflicht, wahrheitsgemäß und genau zu berichten. Sämtliche Auditfeststellungen, Auditschlussfolgerungen und Auditberichte müssen die Audittätigkeit wahrheitsgemäß und genau widerspiegeln. Auch über wesentliche Hindernisse, die während des Audits aufgetreten sind und über nicht bereinigte, auseinandergehende Auffassungen zwischen dem Auditteam und der auditierten Organisation muss berichtet werden. Die Kommunikation muss wahrheitsgetreu, genau, objektiv, zeitgerecht, klar und vollständig (dokumentiert) sein.

4.2.3. Angemessene berufliche Sorgfalt

Angemessene berufliche Sorgfalt bezieht sich auf das Engagement und Urteilsvermögen bei der Durchführung von Audits.

Auditoren haben sorgfältig vorzugehen, entsprechend der Bedeutung der Aufgabe, die sie verrichten und dem Vertrauen, das Viacryp und andere zuständige Parteien in sie setzen. Ein wichtiger Faktor bei der Durchführung ihrer Arbeit mit der entsprechenden beruflichen Sorgfalt ist die Fähigkeit, in allen Situationen, die während eines Audits auftreten, begründete Urteile fällen zu können.

4.2.4. Vertraulichkeit

Es geht hier um die Sicherheit von Informationen. Auditoren müssen bei der Verwendung und dem Schutz von Informationen, die sie im Verlaufe ihrer Aufgaben erworben haben, umsichtig sein. Auditinformationen dürfen nicht unangemessen zur persönlichen Bereicherung des Auditors oder der Organisation, die das Audit anfordert, oder in einer Weise verwendet werden, die nachteilig für die berechtigten Interessen der zu auditierenden Organisation ist. Dieses Konzept schließt den ordnungsgemäßen Umgang mit sensiblen, vertraulichen Informationen ein.

4.2.5. Unabhängigkeit

Unabhängigkeit ist die Grundlage für die Unparteilichkeit des Audits und die Objektivität der Auditschlussfolgerungen. Wenn es praktisch durchführbar ist, haben Auditoren unabhängig von der Aktivität zu sein, die auditiert wird. Auditoren haben in allen Fällen frei von Voreingenommenheit und Interessenkonflikten zu handeln. Hinsichtlich interner Audits haben die Auditoren unabhängig von den zuständigen Managern zu sein, deren Funktion auditiert wird. Auditoren haben während des gesamten Auditprozesses eine objektive Haltung zu bewahren, um zu gewährleisten, dass die Auditfeststellungen und die Auditschlussfolgerungen ausschließlich auf Auditnachweisen beruhen.

4.2.6. Rückführbare Vorgehensweise

Das Ziel ist mithilfe eines systematischen Auditprozesses zu zuverlässigen und nachvollziehbaren Auditschlussfolgerungen zu gelangen. Auditnachweise müssen verifizierbar sein. Sie beruhen in der Regel auf Stichproben aus den verfügbaren Informationen, da ein Audit während eines festgelegten Zeitraums und mit begrenzten Ressourcen durchgeführt wird. Die Stichprobennahme muss bezüglich Umfang und Art angemessen sein, da dies entscheidend für das Vertrauen in die Auditschlussfolgerungen ist.

4.3. Durchführung des Audits

Viacryp lässt das Audit regelmäßig von einer unabhängigen dritten Partei innerhalb eines von Viacryp definierten Rahmens durchführen. Das Ziel des Audits besteht darin, mit einem unabhängigen Expertenurteil die unabhängige und interessenneutrale Position von Viacryp zu bestätigen. Als Trusted Third Party engagiert sich Viacryp als Vermittler zwischen dem/den Lieferanten der originalen personenbezogenen Daten und dem Abnehmer der pseudonymisierten Daten.

Es folgt die Vorgehensweise zur Ausstellung einer Assurance Konformitätserklärung in Grundzügen.

4.4. Aufstellen eines Auditplans

Im Vorfeld der Untersuchungen, wie in Kapitel 2 dargestellt, wird gemeinsam mit der auditierten Organisation (Viacryp) ein Auditplan aufgestellt. Dieser Auditplan muss die folgenden Aspekte umfassen:

- Die Auditziele
- Der Umfang des Audits, einschließlich der Festlegung der zu auditierenden Organisations- und Funktionseinheiten und der Prozesse gemäß denen das Audit durchgeführt wird
- Die Auditkriterien und etwaige Referenzdokumente
- Die Standorte, Termine, voraussichtlichen Zeitpunkte und Dauer der durchzuführenden Audittätigkeiten, einschließlich der Besprechungen mit der Leitung von Viacryp
- Die verwendeten Auditmethode einschließlich des Umfangs, innerhalb dessen Probenahmen beim Audit erforderlich sind, um hinreichende Auditnachweise zu erzielen sowie die Gestaltung des Probenahmeprogramms, soweit zutreffend

- Die Rollen und Verantwortlichkeiten der Auditteammitglieder, Betreuer und Beobachter
- Bereitstellung der erforderlichen Ressourcen für besonders wichtige Teile des Audits
- Ansprechpartner bei dem Beschwerden eingereicht werden können

4.5. Informationen sammeln und verifizieren

Im Verlaufe des Audits müssen Informationen, die für die Auditziele, den Auditumfang sowie die Auditkriterien relevant sind, einschließlich der Informationen, die sich auf Schnittstellen zwischen Funktionsbereichen, Tätigkeiten und Prozessen beziehen, durch angemessene Stichproben gesammelt und verifiziert werden. Ausschließlich verifizierbare Informationen sind als Auditnachweise zu akzeptieren. Auditnachweise, die zu Auditfeststellungen führen, müssen protokolliert werden. Wenn das Auditteam während des Sammelns von Nachweisen erfährt, dass neue oder veränderte Umstände oder Risiken auftreten, sind sie vom Team zu bearbeiten.

Methoden zur Sammlung von Informationen sind beispielsweise:

- Befragungen
- Beobachtungen
- Auswertung von Dokumenten, einschließlich Protokollen

4.6. Auditfeststellungen formulieren

Auditnachweise müssen anhand von Auditkriterien ausgewertet werden, um zu Auditfeststellungen zu gelangen. Auditfeststellungen können auf Konformität oder Abweichungen bezüglich der Auditkriterien hinweisen. Wenn das im Auditplan spezifiziert wurde, müssen die einzelnen Auditfeststellungen auch Konformität und „Good Practices" mit den entsprechenden Nachweisen, Verbesserungsmöglichkeiten und etwaige Empfehlungen für die auditierte Organisation umfassen.

Abweichungen und die entsprechenden Nachweise müssen protokolliert werden. Die Erfassung einer Abweichung durch den Auditor erfolgt gemäß dem Anforderung-Abweichung-Nachweis-Prinzip. Abweichungen können klassifiziert werden. Abweichungen müssen mit der auditierten Organisation besprochen werden, um sicherzustellen, dass die Auditnachweise zutreffend sind und dass die Abweichungen nachvollzogen werden können. Man muss sich optimal dafür einsetzen, etwaige auseinandergehende Auffassungen bezüglich der Auditnachweise oder der Auditfeststellungen zu bereinigen und nicht bereinigte Probleme sind aufzuzeichnen. Wenn Abweichungen angetroffen werden, gliedert der Prüfungsrahmen die Feststellungen in zwei Gruppen:

- Nichtkonformität: eine erhebliche Nichterfüllung der Auditanforderungen. Wenn eine oder mehrere Nichtkonformitäten vorliegt bzw. vorliegen, müssen sie behoben werden, ansonsten kann das Audit nicht mit einem positiven Ergebnis abgeschlossen werden.
- Empfehlung: Sie stützt sich auf eine Wahrnehmung des Auditors, die sich auf mögliche Verbesserungspotentiale oder Optimierungen, jedoch nicht auf Auditanforderungen bezieht. Empfehlungen führen damit nicht zu Nichtkonformitäten.

Bei der Überprüfung können mehr oder weniger erhebliche Defizite gemeldet werden. Abhängig von der Schwere der gemeldeten Defizite wird der Auditor feststellen, ob es sich um eine wesentliche oder untergeordnete Nichtkonformität (Kategorisierung der Erkenntnisse) handelt. Untergeordnete Nichtkonformitäten gehen in der Regel mit begrenzten Risiken einher. Mehrere untergeordnete Nichtkonformitäten können vom Auditor einer wesentlichen Nichtkonformität gleichgestellt werden und zwar auf Grundlage seines professionellen Urteilsvermögens unter Berücksichtigung der Schwere der Abweichung. Sowohl untergeordnete Nichtkonformitäten wie auch wesentliche Nichtkonformitäten sind innerhalb von 13 Wochen, mit Nachweisen belegbar, zu beheben.

Hinsichtlich jeder Empfehlung wird Viacryp abwägen, ob ein dementsprechender Handlungsbedarf besteht oder nicht.

4.7. Weiterverfolgung der Auditschlussfolgerungen (Follow-up-Audit)

Abhängig von den Auditzielsetzungen können die Schlussfolgerungen des Audits darauf hinweisen, dass Korrekturen bzw. Korrektur- oder Vorbeugungsmaßnahmen oder Verbesserungsmaßnahmen erforderlich sind. Üblicherweise fasst die auditierte Organisation einen Beschluss zu diesen Maßnahmen und setzt sie innerhalb eines vereinbarten Zeitrahmens um. Die auditierte Organisation muss die Person, die das Auditprogramm leitet und das Auditteam gegebenenfalls über den Status dieser Maßnahmen auf dem Laufenden halten. Der Abschluss und die Wirksamkeit dieser Maßnahmen müssen verifiziert werden. Diese Verifizierung kann Teil eines Follow-up-Audits sein.

4.8. Auditbericht

Von der ersten Beurteilung wird ein Auditbericht gemäß der Risk Based Certification™ MSC Berichtlegung der DNV GL erstellt. Darin können Möglichkeiten zur Verbesserung und positive Feststellungen aufgenommen werden. In dem Bericht stehen jedoch keine spezifischen Lösungen. Der Bericht ist eine deutliche und kurz gefasste Darstellung der durchgeführten Untersuchung. Aus dieser Darstellung muss eindeutig hervorgehen, ob das entsprechende Audit mit einem positiven Ergebnis abgeschlossen wurde.

Der Auditbericht muss das Audit umfassend, genau, kurz gefasst und eindeutig wiedergeben. Er muss die folgenden Aspekte umfassen oder darauf hinweisen:

a. Die Auditzielsetzungen
b. Der Umfang des Audits, im Besonderen die Festlegung der zu auditierenden Organisations- und Funktionseinheiten und Prozesse gemäß denen das Audit durchgeführt wird
c. Festlegung des Auditkunden
d. Festlegung des Auditteams und der Teilnehmer der auditierten Organisation am Audit
e. Die Termine und Standorte an denen die Audittätigkeiten durchgeführt wurden
f. Die Auditkriterien
g. Die Auditfeststellungen und die entsprechenden Nachweise
h. Die Auditschlussfolgerungen
i. Eine Erklärung in der steht, inwieweit die Auditkriterien erfüllt wurden

Der Untersuchungsbericht wird mit Viacryp abgestimmt und er wird in seiner endgültigen Form ausschließlich Viacryp zur Verfügung gestellt. Es liegt im Ermessen von Viacryp, ob er dem Abnehmer bereitgestellt wird. Viacryp und der Abnehmer können den Assurance-Bericht und den zugehörigen Bericht der niederländischen Aufsichtsbehörde CBP zum Nachweis ihrer Konformität anbieten. Die Parteien dürfen den Assurance-Bericht beispielsweise auf ihrer Website veröffentlichen. Letzteres gilt nicht für den zugehörigen Auditbericht. Der Auditbericht darf anderen Parteien ausschließlich nach vorheriger Abstimmung mit dem Auditor zur Verfügung gestellt werden.

Anlage A.1 Abkürzungen und Definitionen

Es folgt eine Liste mit Abkürzungen, die in diesem Dokument eingesetzt werden samt der entsprechenden Bedeutung:

Abkürzung	Bedeutung
AP	Niederländische Aufsichtsbehörde für den Datenschutz: Autoriteit Persoonsgegevens
AVG	Niederländisches Datenschutzgesetz: Algemene Verordening Gegevensbescherming
CBP	Niederländische Aufsichtsbehörde für den Datenschutz: College Bescherming Persoonsgegevens (frühere Bezeichnung der Autoriteit Persoonsgegevens)
DSGV	Datenschutz-Grundverordnung, europäisches Gesetz, das ab dem 25. Mai 2018 die Datenschutzgesetze der einzelnen Mitgliedsstaaten ersetzt
GDPR	General Data Protection Regulation, englische Bezeichnung für die DSVG
ISO	International Organization for Standardization
SOA	Statement of Applicability, auch Anwendbarkeitserklärung genannt
TTP	Trusted Third Party
WBP	Niederländisches Datenschutzgesetz: Wet bescherming persoonsgegevens
XML	Extensible Markup Language

Ferner folgt hier eine Liste mit Definitionen und der zugehörigen Beschreibung:

Begriff	Beschreibung
Abnehmer	Partei, die die von Viacryp pseudonymisierten Daten nutzt.
Abweichung	Nichterfüllung einer Anforderung.
Anbieter	Partei, die personenbezogene Daten an Viacryp liefert.
Anonymisieren	Der Prozess bei dem der Bezug zwischen den personenbezogenen Daten und dem jeweiligen Individuum entfernt wird.
Anwendbarkeitserklärung	Dokument, in dem dargestellt wird, welche Maßnahmen im Rahmen des NEN-ISO 27002 „Leitfaden für Informationssicherheit" und SOA ISO 27001 ergriffen wurden.
Auditfeststellungen	Ergebnisse aus der Bewertung der gesammelten Auditnachweise im Hinblick auf die Auditkriterien.
Auditierte Organisation	Organisation, die einem Audit unterzogen wird.
Auditkriterien	Satz an Richtlinien, Verfahren oder Anforderungen, die als Bezugsgrundlage zur Prüfung der Auditnachweise herangezogen werden.
Auditkunde	Organisation oder Person, die ein Audit beantragt.

Begriff	Beschreibung
Auditnachweise	Aufzeichnungen, Tatsachenfeststellungen oder andere Informationen, die für die Auditkriterien relevant und verifizierbar sind.
Auditor	Person, die ein Audit durchführt.
Auditplan	Beschreibung der Tätigkeiten und Einrichtungen für ein Audit.
Audits	Systematische, unabhängige und dokumentierte Prozesse zur Erlangung von Auditnachweisen und deren objektiver Auswertung, um zu ermitteln, inwieweit die vereinbarten Auditkriterien erfüllt sind. Audits werden in diesem Dokument in drei Typen gegliedert und zwar: (1) Anfangsbeurteilung (auch Anfangsaudit genannt): Dabei handelt es sich um die ersten Audits, die sich auf den Aufbau und das Vorhandensein von Maßnahmen in Übereinstimmung mit den Viacryp-Kriterien konzentrieren; (2) Wiederholungsuntersuchung: Dabei handelt es sich um Audits, die jährlich durchgeführt werden nachdem das Anfangsaudit durchgeführt worden ist, auch als Wiederholungsaudits bekannt, die sich auf die Wirksamkeit der Maßnahmen konzentrieren, die im Rahmen der Anfangsbeurteilung im Laufe der vergangenen Frist untersucht wurden und (3) Follow-up-Untersuchung: Audits bezüglich der Korrekturmaßnahmen aus Anlass der bei dem Anfangsaudit oder den jährlichen Audits festgestellten Nichtkonformitäten; (4) Neubeurteilung: Dabei handelt es sich um ein Audit, das durchgeführt wird, wenn sich der Untersuchungsgegenstand erheblich ändert.
Auditschlussfolgerung	Ergebnis eines Audits, nach Erwägung der Auditzielsetzungen und aller Auditfeststellungen.
Auditteam	Ein Auditor oder mehrere Auditoren, der/die ein Audit durchführt/durchführen, bei Bedarf mit der Unterstützung eines technischen Sachverständigen.
Auditumfang	Anwendungsbereich und Grenzen eines Audits.
Beobachter	Person, die das Auditteam begleitet, jedoch keine Audits durchführt.
Betreuer	Person, die von der auditierten Organisation mit der Unterstützung des Auditteams beauftragt wurde.
Chinese Wall	Trennung zwischen den pseudonymisierten Daten und den sonstigen Daten.
Delivery-Modul	Zielmodul zur Bereitstellung der Daten beim Abnehmer.
Kompetenz	Das Vermögen, Fähigkeiten und Fertigkeiten zur Erzielung der angestrebten Ergebnisse einzusetzen.
Konformität	Erfüllung einer Anforderung.
Kunden	Kombination aus Anbietern und Abnehmern innerhalb einer Viacrypstraße.
Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels

Begriff	Beschreibung
	Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (AVG Art. 4, Absatz 1).
Pseudonymisieren	Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (AVG Art.1, Absatz 5).
Pseudonymizer	Zentrales Modul TTP innerhalb dessen die Pseudonymisierung der Daten stattfindet.
Replay Attack	Der unrechtmäßige Zugriff auf ein Informationssystem mit der Absicht, einen Einblick in den Bezug zwischen personenbezogenen Daten und den eingesetzten Pseudonymen zu erhalten.
Risiko	Auswirkung der Unsicherheit hinsichtlich der Erreichung der Zielsetzungen.
Supply Modul	Versandmodul für den Anbieter, innerhalb dessen die Spaltung der Daten wie auch der verschlüsselte Versand der Daten stattfindet.
Technischer Sachverständiger	Person, die dem Auditteam mit spezifischen Fachkenntnissen zur Seite steht.
Untergeordnete Nichtkonformität	Ein geringfügiges Defizit im Hinblick auf die Viacryp Kriterien.
Verarbeiten	Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (AVG Art. 1, Absatz 2).
Viacrypstraße	Jede Straße umfasst einen oder mehrere Anbieter personenbezogener Daten und einen Abnehmer der pseudonymisierten Ergebnisse. Viacryp kümmert sich dabei um die Pseudonymisierung der personenbezogenen Daten, die von dem oder den Anbieter(n) stammen und stellt sie dem Abnehmer bereit.
Wesentliche Nichtkonformität	Ein erhebliches Defizit im Hinblick auf die Viacryp Bedingungen. Wenn den Viacryp-Kriterien nicht entsprochen wird, handelt es sich um eine wesentliche Nichtkonformität. Wenn eine oder mehrere Nichtkonformitäten vorliegen, sind sie zu beheben, ansonsten kann das Audit nicht mit einem positiven Ergebnis abgeschlossen werden.

Anlage A.2 Einzusetzende Kontrollziele für das Audit-Rahmenwerk

ISO 27001:2013

A.9.1 Geschäftsanforderungen an die Zugangssteuerung
Zielsetzung:
Zugang zu Informationen und informationsverarbeitenden Einrichtungen begrenzen.

A.9.1.1 Zugangssteuerungsrichtlinie
Maßnahme:
Eine Richtlinie zur Zugangssteuerung muss auf Grundlage der Geschäfts- und Informationssicherheitsanforderungen festgelegt, dokumentiert und beurteilt werden.

A.10.1 Kryptographische Maßnahmen
Zielsetzung:
Schutz der Vertraulichkeit, Authentizität und Integrität der Information mithilfe kryptographischer Mittel.

A.10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen
Maßnahme:
Zum Schutz von Informationen muss eine Richtlinie zum Gebrauch von kryptografischen Maßnahmen entwickelt und implementiert werden.

A.10.1.2 Schlüsselverwaltung
Maßnahme:
Bezüglich der Nutzung, des Schutzes und der Lebensdauer von kryptografischen Schlüsseln muss während ihres gesamten Lebenszyklus eine Richtlinie entwickelt und implementiert werden.

A.12.1 Betriebsabläufe und -verantwortlichkeiten
Zielsetzung:
Den ordnungsgemäßen und sicheren Betrieb von informationsverarbeitenden Einrichtungen sicherstellen.

A.12.1.2 Änderungssteuerung
Maßnahme:
Änderungen der Organisation, der Geschäftsprozesse, an den informationsverarbeitenden Einrichtungen und Systemen, die die Informationssicherheit beeinflussen, werden gesteuert.

A.12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen
Maßnahme:
Entwicklungs-, Test- und Betriebsumgebungen müssen voneinander getrennt sein, um das Risiko des unbefugten Zugangs zur oder unbefugter Änderungen an der Betriebsumgebung zu senken.

A.12.3 Datensicherung
Zielsetzung:
Schutz vor Datenverlust.

A.12.3.1 Sicherung von Information
Maßnahme:
Regelmäßig müssen Sicherungskopien von Informationen, Software und Systemabbildungen in Übereinstimmung mit der vereinbarten Richtlinie zur Datensicherung erstellt und getestet werden.

A.12.4 Protokollierung und Überwachung
Zielsetzung:
Ereignisse protokollieren und Nachweise sammeln.

A.12.4.1 Ereignisprotokollierung
Maßnahme:
Es sind Ereignisprotokolle anzufertigen, aufzubewahren und regelmäßig zu überprüfen, in denen Tätigkeiten der Benutzer, Ausnahmen und Informationssicherheitsereignisse aufgezeichnet werden.

A.12.4.2 Schutz der Protokollinformationen
Maßnahme:
Protokollierungseinrichtungen und Protokollinformationen müssen vor Manipulation und unbefugtem Zugriff geschützt werden.

A.12.4.3 Administratoren- und Bedienerprotokolle
Maßnahme:
Es sind Protokolle der Tätigkeiten von Systemadministratoren und Systembediener anzufertigen, zu schützen und regelmäßig zu überprüfen.

A.13.2 Informationsübertragung
Zielsetzung:
Die Sicherheit von übertragenen Informationen und Programmen, sowohl innerhalb einer Organisation als auch mit jeglicher externen Organisation sicherstellen.

A.13.2.1 Richtlinien und Verfahren zur Informationsübertragung
Maßnahme:
Zum Schutz der Informationsübertragung, die über alle Arten von Kommunikationseinrichtungen verläuft, müssen formale Richtlinien, Verfahren und Kontrollmaßnahme bezüglich der Übertragung gelten.

A.13.2.2 Vereinbarungen zur Informationsübertragung
Maßnahme:
Die Vereinbarungen müssen sich auf die gesicherte Übertragung der Geschäftsinformationen zwischen der Organisation und externen Parteien beziehen.

A.13.2.3 Elektronische Nachrichtenübermittlung
Maßnahme:
Informationen, die auf elektronischem Wege übermittelt werden, müssen angemessen geschützt werden.

A.13.2.4 Vertraulichkeits- und Geheimhaltungsvereinbarungen
Maßnahme:
Anforderungen an die Vertraulichkeits- und Geheimhaltungsvereinbarungen, die den Bedürfnissen der Organisation bezüglich des Schutzes der Informationen entsprechen, müssen festgelegt, regelmäßig überprüft und dokumentiert werden.

A.15.1 Informationssicherheit in Lieferantenbeziehungen
Zielsetzung:
Den Schutz von Betriebsmitteln der Organisation, die für Lieferanten zugänglich sind, gewährleisten.

A.15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen
Maßnahme:
Mit dem Lieferanten müssen die Informationssicherheitsrichtlinien zur Senkung von Risiken, die im Zusammenhang mit dem Zugang des Lieferanten zu den Betriebsmitteln der Organisation stehen, vereinbart und dokumentiert werden.

A.16.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen
Zielsetzung:
Eine konsistente und wirksame Herangehensweise für die Handhabung von Informationssicherheitsvorfällen einschließlich der Benachrichtigung über Sicherheitsereignisse und Schwachstellen.

	A.16.1.2 Meldung von Informationssicherheitsereignissen **Maßnahme:** Informationssicherheitsereignisse sind so schnell wie möglich über geeignete Kanäle zu deren Handhabung zu melden.
ISO20000-1	8.1 Vorfallsmanagement 8.2 Problemmanagement 9.1 Konfigurationsmanagement 9.2 Änderungsmanagement

Anlage A.3 Indikative Liste der Themen je Untersuchung

Untersuchung	Möglicherweise festzustellende Defizite
1	• Es wird keine Pseudonymisierung eingesetzt. • Private Keys werden nicht wirklich von den Inhabern erstellt. • Der Aufbau der Pseudonymisierung entspricht nicht dem „Good Practice“ der Verschlüsselungstechnologie (unzureichend fachkundig). • Der erste Schritt der Verschlüsselung findet nicht beim Anbieter der Daten statt. • Der erste Schritt der Verschlüsselung ist ohne Hinzuziehung zusätzlicher Informationen umkehrbar. • Die Pseudonymisierung ist nicht angemessen im Code implementiert. • Die implementierte Lösung stimmt nicht mit der dargestellten Lösung überein. • Es wurde kein Managementprozess eingerichtet. • Der Managementprozess weist Defizite auf. • Die Art und Weise, wie die Organisation Kenntnisse zu aktuellen Entwicklungen auf dem Gebiet der Verschlüsselung und Informationssicherheit sammelt, ist unzureichend oder erfolgt ad hoc.
2	• Die Maßnahmen, die im Rahmen der Informationssicherheit ergriffen wurden, sind derart, dass unbefugte Personen möglicherweise dazu in der Lage sind, die Verschlüsselung rückgängig zu machen. • Die Maßnahmen, die im Rahmen der Informationssicherheit ergriffen wurden, sind derart, dass unbefugte Personen (in böser Absicht) möglicherweise dazu in der Lage sind, die Verschlüsselung rückgängig zu machen. • Die Vereinbarungen mit dem Hosting-Lieferanten sind unzureichend klar oder werden nicht überprüft.
3	• Die allgemeinen Bedingungen sind unzureichend spezifisch. • Es wurden keine Vereinbarungen zur Auftragsdatenverarbeitung mit Kunden abgeschlossen. • Es wurden keine umfassenden Vereinbarungen zwischen Anbieter und Abnehmer mit Viacryp getroffen.

Anlage A.4 Verschlüsselungstechniken

Typ	Algorithmus
Asymmetrische Verschlüsselung	RSA-2048
Symmetrische Verschlüsselung	AES-256-GCM
Signing	SHA-256 with RSA
Hashing	HMAC-SHA-512