Data Privacy Certificate

Prüfbericht

ausgestellt durch:

DATA TRUST CENTER

zertifiziertes Unternehmen:

adpublisher AG

7. September 2017

Inhaltsverzeichnis

A. Data Privacy Certificate

Geprüfter Sachverhalt:

Das Geschäftsmodell der adpublisher AG besteht darin, über Gewinnspiele (online und offline) und andere Kontaktmöglichkeiten sog. Leads für Unternehmen zu generieren. Mit Hilfe dieser Leads ist dann das jeweilige Unternehmen in der Lage, seine Kunden gezielt zu kontaktieren oder neue Kunden zu akquirieren und Produkte anzupreisen.

Bei der Teilnahme an einem Gewinnspiel oder anderen Kontakten durchläuft der Teilnehmer das sog. Double-Opt-In Verfahren, mit Hilfe dessen jeder Teilnehmer seine Teilnahme an einem Gewinnspiel oder die Zustimmung zu weiteren Kontakten unmissverständlich erklärt und gegenüber der adpublisher AG bestätigt. Beim Double-Opt-In Verfahren handelt es sich um ein zweistufiges Verfahren, bei dem der Teilnehmer in einem ersten Schritt seine E-Mail Adresse in einem dafür vorgesehenen Feld einträgt. Das System verschickt daraufhin ein sogenanntes Bestätigungs-E-Mail an die vom Teilnehmer angegebene E-Mail Adresse. Über das Aktivieren eines weiteren Links bestätigt der Teilnehmer, dass eine bestimmte E-Mail Adresse besteht und dass er damit einverstanden ist, von einem bestimmten Unternehmen (einem Kunden der adpublisher AG) kontaktiert zu werden (Datenschutzbestimmungen und Teilnahme-bedingungen).

Die bei Gewinnspielen generierten Daten werden im Auftrag der adpublisher AG bei einem technischen Dienstleister, der als Datawarehouse Host agiert (z.B. MMP Services GmbH = Datawarehouse) und mit Hilfe einer speziellen Software (z.B. Coyote Software = Host) in Deutschland gespeichert. Die adpublisher AG speichert selbst keine der generierten Daten, hat jedoch jederzeit Zugriff auf diese Daten.

Bei den Kunden der adpublisher AG handelt es sich um Unternehmen, die entweder direkt über die adpublisher AG ein Gewinnspiel für ihre Zwecke bauen lassen (z.B. Tchibo GmbH); oder es handelt sich um Unternehmen, die ihrerseits

einen Dienstleister mit der Durchführung einer Werbekampagne und/oder der Durchführung eines Gewinnspiels beauftragen. Dieser Dienstleister (z.B. Global Group Dialog Solutions GmbH), der in diesem Fall zwischen das Unternehmen und die adpublisher AG geschaltet ist, betreibt für das Unternehmen ein Gewinnspiel. Es gibt jedoch auch Kunden, meist handelt es sich dabei um kleinere Unternehmen, die ein bereits bestehendes Gewinnspiel bei einem Webbetreiber (Publisher) sponsern wollen. In einem solchen Fall erteilt ein Unternehmen der adpublisher AG einen entsprechenden Auftrag über die Generierung von Leads (AGB Kunden).

Ein Publisher, der Webseiten betreibt und auf diesen Seiten Werbeflächen z.B. in der Form von Bannern der adpublisher AG für ihre Kunden zur Verfügung stellt, meldet sich auf der Homepage der adpublisher AG als Publisher an. Wird der Antragsteller als Publisher seitens der adpublisher AG akzeptiert, werden für dieses Vertragsverhältnis die auf der Homepage der adpublisher AG zur Verfügung gestellten und abrufbaren AGBs Vertragsbestandteil (AGB Publisher).

Wünscht ein Teilnehmer eines Gewinnspiels nicht mehr von der adpublisher AG oder einem Kunden der adpublisher AG kontaktiert zu werden, so hat er ein jederzeitiges Widerrufsrecht und stellt die adpublisher AG über ein spezielles Verfahren (Aufnahme in eine Blacklist) sicher, dass dieser Teilnehmer für zukünftige Gewinnspiele oder Kontaktaufnahmen gesperrt ist.

Umfang der rechtlichen Prüfung:

Der Umfang der rechtlichen Prüfung umfasst die im Zusammenhang mit obigem Sachverhalt den Prüfern übergebenen und unten im Detail aufgeführten Dokumente. Bei diesen Dokumenten handelt es sich betreffend den Prüfungsumfang um Beispiele der verschiedenen in Verwendung befindlichen Verträge, die sich jedoch nicht als abschliessend versteht.

Die adpublisher AG erklärt, rechtlich und technisch in Einklang mit den Internationalen Datenschutzbestimmungen (International Data Privacy Principles)

zu handeln. Dies wurde vom DATA TRUST CENTER stichprobenweise überprüft und nach Massgabe der Prüfungsergebnisse als zutreffend befunden.

Das DATA TRUST CENTER erteilt daher nach durchgeführter Prüfung der adpublisher AG das International Data Privacy Certificate.

Dies berechtigt die adpublisher AG, das Data Privacy Certificate sowie das Siegel öffentlich zu führen und damit zu werben. Die adpublisher AG ist verpflichtet, den Prüfbericht bei Verlangen (anonymisiert) offenzulegen bzw. auf ihrer Homepage darauf zu verweisen und entsprechend online zur Verfügung zu stellen.

Vaduz/Ruggell, 7. September 2017

Jürgen Winkler *Claudia Rigon*
für die adpublisher AG

ao. Univ.-Prof. Dr. Wolfgang Zankl
für die Juranovit Forschungs GmbH

Mag. iur. Stefan Ritter
für die ky-center ag
for social media law

Sven Durgiai
für die Kyberna AG

B. Zertifizierer und Zertifizierungsgegenstand

1. Allgemein

Das DATA TRUST CENTER ist ein Joint Venture der ky-center ag for social media law, der Kyberna AG und der Juranovit Forschungs GmbH. Es hat auf Basis der Forschungen von ao. Univ.-Prof. Dr. Wolfgang Zankl Internationale Datenschutzbestimmungen (International Data Privacy Principles) entwickelt, die auf technischen und rechtlichen Standards sowie insbesondere auch auf einem Ansatz normativer Leistungsäquivalenz und der Berücksichtigung europäischer, US-amerikanischer, asiatischer und internationaler Data Privacy Standards beruhen.

2. Rechtlich

Die rechtliche Prüfung wird auf Basis der zum Zeitpunkt der Prüfung geltenden Internationalen Datenschutzbestimmungen (Stand April 2017) durchgeführt:

Diese lauten wie folgt:
Unternehmen, die im Einklang mit den Internationalen Datenschutzbestimmungen handeln, verpflichten sich:

1. zur Einhaltung der nationalen Gesetze betreffend die Datensicherheit und den Datenschutz sowie dazu, die nationalen Bestimmungen betreffend das Vertragsrecht und andere rechtliche Vorschriften des Datenschutzes einzuhalten;

2. zur Einhaltung der geltenden Sicherheitsstandards, um gespeicherte Personendaten vor unerlaubtem, rechtswidrigem oder auch nur zufälligem Zugriff, Verarbeitung, Löschung, Verlust oder Verwendung zu schützen;

3. eine einfach erkennbare, zugängliche und verständliche Datenschutzrichtlinie einzuführen, die Informationen über diejenige Person enthält, die im

Unternehmen für den Datenschutz verantwortlich ist sowie Informationen darüber, wie diese Person persönlich kontaktiert werden kann, über die Gründe, weshalb persönliche Daten gesammelt werden, um welche Daten es sich dabei handelt und wie diese Daten benützt werden sowie darüber, wer Zugang zu diesen Daten hat, wie lange diese Daten gespeichert werden, ob und welche Daten wann gelöscht werden und ob diese auf Verlangen hin richtig gestellt werden;

4. zur Schulung der Mitarbeiter betreffend die Einhaltung des Datenschutzes und dazu, Handlungen zu vermeiden, die den gemäss Punkt 2. unerlaubten oder rechtswidrigen Zugriff auf Daten ermöglichen bzw. begünstigen könnten;

5. die Daten nicht für andere Zwecke zu verwenden oder zu verarbeiten als wozu das Unternehmen gesetzlich verpflichtet oder vom Kunden ausdrücklich autorisiert worden ist. Ausgenommen hiervon ist die Nutzung für statistische Zwecke, sofern es sich um anonymisierte Daten handelt.

6. keine Kundendaten zu sammeln, soweit dies nicht notwendig oder übermässig ist;

7. zum Gebrauch und zur Verbreitung von Kundendaten in einer angemessenen Art und Weise sowie nur für Zwecke, die mit dem Gegenstand des Unternehmens zusammenhängen;

8. keine Kundendaten an Dritte zu übermitteln, ausser diese Dritten verpflichten sich (ebenfalls) dazu, die vorliegenden oder vergleichbare Datenschutzbestimmungen einzuhalten.

9. zur Bekanntgabe von Datenpannen soweit es sich um sensible Daten handelt (zum Beispiel in Bezug auf sexuelle, finanzielle, medizinische, politische, ethnische oder religiöse Bereiche);

10. dazu, persönliche Daten nicht länger als notwendig aufzubewahren;

11. dazu, keine persönlichen Daten in Staaten mit unzureichenden oder unbekannten Datenschutzstandards weiterzuleiten, ausser der Kunde wird darüber informiert, dass die Standards in diesem Staat unzulänglich oder unbekannt sind und er einer solchen Übermittlung ausdrücklich zustimmt;

12. für den Fall, dass zwischen dem Kunden und dem Unternehmen ein Vertragsverhältnis besteht, das den Kunden verpflichtet, ein Entgelt für Dienstleistungen oder Waren zu leisten, dazu:

    - den Kunden im Falle einer Datenpanne persönlich und so rasch als vernünftigerweise möglich darüber und die betroffenen persönlichen Daten zu informieren;

    - den Kunden auf seine Anfrage hin darüber zu informieren, welche spezifischen Daten gespeichert oder gelöscht werden und darüber, ob es zwingende Gesetze oder Bestimmungen gibt, die verlangen, dass das Unternehmen die Daten weiter speichert;

    - inhaltsbezogene persönlichen Daten nicht zu gebrauchen oder zu verbreiten;

    - keine anderen persönlichen Daten zu gebrauchen oder zu verbreiten, ohne vom Kunden die ausdrückliche, separate und individuell erteilte Zustimmung einzuholen;

    - keine Kundendaten zu speichern, zu gebrauchen oder zu verbreiten, wenn das gesamte Entgelt oder Teile des vom Kunden geleisteten Entgelts dafür bezahlt wird, dass das Unternehmen die Daten nicht speichert, benützt oder verbreitet, ausser es gibt Gesetze oder Bestimmungen, die das Unternehmen dazu verpflichten.

13. für den Fall, dass zwischen dem Kunden und dem Unternehmen ein Vertragsverhältnis besteht, das den Kunden nicht verpflichtet, ein Entgelt für Dienstleistungen oder Waren zu leisten, dazu:

    - den Kunden im Falle einer Datenpanne so rasch als vernünftigerweise möglich betreffend sensible Daten zu informieren;

    - den Kunden auf seine Anfrage hin darüber zu informieren, welche spezifischen sensiblen Daten gespeichert werden und solche Daten auf Verlangen des Kunden zu löschen, wenn diese Daten veraltet sind. Ausgenommen davon sind Datensätze, die aufgrund zwingender Gesetze oder Bestimmungen weiter gespeichert werden müssen;

    - keine sensiblen Daten zu gebrauchen oder zu verbreiten, ohne vom Kunden die ausdrückliche, separate und individuell erteilte Zustimmung einzuholen.

3. Technisch

Die technische Prüfung im Sinne des Punktes (2) der Internationalen Datenschutzbestimmungen wird auf Basis der ISO 27001 durchgeführt, wobei – keine ISO-Zertifizierung ieS erfolgt – nicht sämtliche Voraussetzungen und Schritte des entsprechenden Verfahrens eingehalten werden müssen, sondern ISO 27001 die Grundlage darstellt, an der sich die technische Prüfung orientiert.

C. Prüfungs- und Zertifizierungsgrundsätze

1. Allgemein

Die Prüfung erfolgt summarisch und stichprobenweise. Eine abschliessende Prüfung erfolgt nicht. Die Prüfung bzw ihre Zertifizierung begründet daher weder eine Haftung gegenüber dem Geprüften noch gegenüber Dritten.

Die Prüfung wurde in rechtlicher Sicht von der ky-center ag for social media law sowie von der Juranovit Forschungs GmbH, in technischer Sicht von der Kyberna AG, durchgeführt.

2. Grundlagen

a) Rechtlich

Der rechtlichen Prüfung wurden folgende von der adpublisher AG zur Verfügung gestellte Dokumente zugrunde gelegt:

- AGB Kunden der adpublisher AG;
- AGB der adpublisher AG online.
- Datenschutzerklärung online
- Vertrag zwischen der adpublisher AG und der MMP Services GmbH
- Vertrag zwischen der adpublisher AG und der Global Group Dialog Solutions AG;
- Vertrag zwischen der adpublisher AG und der Tchibo GmbH;
- Vertrag zwischen der adpublisher AG und der nitramIT GmbH;

b) Technisch

Bei der technischen Prüfung ging es darum die sinnvolle Umsetzung einer Sicherheitsrichtlinie festzustellen. Der technischen Prüfung wurden folgende Kontrollen zugrunde gelegt:

Die Prüfung erfolgt summarisch und stichprobenweise. Eine abschliessende Prüfung erfolgte für technische Belange am 24.05.2017.

Bei der technischen Prüfung ging es darum die sinnvolle Umsetzung einer Sicherheitsrichtlinie festzustellen. Der technischen Prüfung wurden folgende Kontrollen zugrunde gelegt, dies sind gleichzeitig auch die Basisdokumente für die Zertifizierung nach Data Trust Center:

- Informationssicherheitsleitlinie
  - Anhang Informationssicherheitsleitlinie Liste rechtlicher, amtlicher Anforderungen
- Kennwort Richtlinie
- Zugangskontrollrichtlinie
- Notfallwiederherstellungsplan
- Sicherheitsrichtlinie für Lieferanten
  - Anhang Sicherheitsklauseln für Lieferanten und Partner
- Plan für Risikobehandlung
  - Inventar der Werte
  - Verzeichnis Risikoeinschätzung
  - Bericht zur Risikoeinschätzung und Risikobehandlung
  - Risikobewertung
  - Plan zur Risikobehandlung
- Verfahren zum Vorfallsmanagement

Die Prüfung sucht nach nachweisbaren und dokumentierten Sicherheitsrichtlinien und bewertet diese nach folgenden Gesichtspunkten:

- Wurden Anforderungen an den Prüfpunkt definiert?
- Wurde ein Risikomanagement betrieben?
- Wurden Kontrollmechanismen definiert?
- Wird eine Sicherheitsmassnahme im Betrieb umgesetzt?
- Wird eine Sicherheitsmassnahme geprüft?
- Wurde aus den internen Prüfungen Daten gezogen und verarbeitet?
- Wurde ein Verbesserungspotenzial aus einer internen Prüfung abgeleitet?

Sollte einer der Prüfpunkte nachweisbar dokumentiert oder implementiert sein, gilt der Inhaltspunkt als erfüllt. Der Zertifikatsaussteller behält sich das Recht vor, Punkte für angemessen erledigt zu erklären, wenn ein Prüfpunkt erkennbar ist.

D. Prüfungsergebnis

1. Rechtlich

Die adpublisher AG erklärt und bestätigt mit ihrer Unterschrift, die vom DATA TRUST CENTER entwickelten und der gegenständlichen Prüfung zugrunde gelegten Internationalen Datenschutzbestimmungen einzuhalten.

Das DATA TRUST CENTER hat überprüft, ob und inwieweit dies zutrifft.

Die Erklärung der adpublisher AG ist auf Basis der eingesehenen Unterlagen und durchgeführten Kontrollen zutreffend. Es wurden keine gravierenden Verletzungen der Internationalen Datenschutzbestimmungen festgestellt. Auf die Einhaltung der erwähnten Punkte 1., 2. und 3. der Internationalen Datenschutzbestimmungen wird hingewiesen.

Im Einzelnen sind bei Berücksichtigung des erwähnten Hinweises 11 der 13 juristischen Punkte und damit 84,6 % auf Basis der durchgeführten Stichproben als vollständig erfüllt anzusehen. Nur in Bezug auf die unten angefügten Punkte wurden Abweichungen von den Internationalen Datenschutzbestimmungen festgestellt:

a) Gesetzliche oder vertragliche Verwendung der Daten

Punkt 5. ... die Daten nicht für andere Zwecke zu verwenden oder zu verarbeiten als wozu das Unternehmen gesetzlich verpflichtet oder vom Kunden ausdrücklich autorisiert worden ist. Ausgenommen hiervon ist die Nutzung für statistische Zwecke, sofern es sich um anonymisierte Daten handelt.

Datenschutzerklärung online
Ergibt sich (im Zusammenhang mit der Weitergabe von Daten, nicht aber in Bezug auf eigene Nutzung) aus „Werden die erhaltenen Informationen weitergegeben?/Mit Ihrer Einwilligung".

b) Transparenz der Weitergabe von Daten

Punkt 8. ... keine Kundendaten an Dritte zu übermitteln, ausser diese Dritten verpflichten sich (ebenfalls) dazu, die vorliegenden oder vergleichbaren Datenschutzbestimmungen einzuhalten.

Datenschutzerklärung online
„Bei jeder Weitergabe von Daten und Informationen stellt adpublisher sicher, dass die Weitergabe stets in Übereinstimmung mit dieser Datenschutzerklärung erfolgt" („Werden die erhaltenen Informationen weitergegeben?/Mit Ihrer Einwilligung"). Dieser Punkt wäre demnach erfüllt, soweit die Datenschutzerklärung den Internationalen Datenschutz-bestimmungen angepasst wird.

Vertrag zwischen der adpublisher AG und der Global Group Dialog Solutions AG;

Sinngemäss ergibt sich dies aus § 2 (3) -indem festgehalten wird, dass eine Verwendung für andere Zwecke, worunter auch die Weitergabe an Dritte gesehen werden kann, nicht erlaubt ist. Der Vollständigkeit halber wird jedoch angeregt, diesen Passus noch expliziter zu fassen und auch die Weitergabe an Dritte – im Sinne der internationalen Datenschutzbestimmungen entsprechend zu regeln. Auch § 7 sieht vor, dass die Global Group Dialog Solutions Agentur berechtigt ist, Arbeiten von Dritten erfüllen zu lassen, wenn zuvor die Zustimmung der adpublisher AG eingeholt wurde. Insofern wäre dieser Punkt erfüllt.

Vertrag zwischen der adpublisher AG und der Tchibo GmbH

Eine solche Verpflichtung fehlt im Rahmenvertrag und müsste Tchibo auferlegt werden.

Vertrag zwischen der adpublisher AG und der nitramIT GmbH;

Eine solche Regelung ist in der vorliegenden Vereinbarung nicht enthalten und müsste noch aufgenommen werden.

2. Technisch

a) Informationssicherheitsleitlinie

Informationsrichtlinie

	20%	40%	60%	80%	100%
Form					
History					
Zielvorgaben und Messungen					
Anforderungen an Informatinssicherheit					
Massnahmen zur Informationssicherheit					
Betriebliches Kontinuitätsmanagement					
Verantwortlichkeiten					
Leitlinien Kommunikation					
Gültigkeiten					
Vorgabe zur Erreichung					

Die Informationssicherheitsleitlinie wurde erstellt und durch die Geschäftsleitung verabschiedet.

Der Punkt gilt als erfüllt.

b) Kennwort Richtlinie:

Kennwort Richtlinie

	20%	40%	60%	80%	100%
Form					
History					
Zweck und Anwendungsbereich					
Pflichten der Anwender					
Verwaltung von Benutzer-Kennworten					
Gültigkeit und Dokumenten-Management					
Vorgabe zur Erreichung					

Das Dokument «Kennwort –Richtlinie» wurde erstellt und lässt sich auf die Unternehmung anwenden.

Der Punkt gilt als erfüllt:

Für das nächste Audit ist vorzulegen:

Liste der Verstösse gegen die Richtlinie	Als Minimum wird empfohlen, eine Excel Datei zu führen die alle Verstösse gegen die Kennwort Richtlinie dokumentiert.

c) Zugangskontrollrichtlinie:

Zugangskontrollrichtlinie

	20%	40%	60%	80%	100%
Form					
History					
Zweck und Anwendungsbereich					
Referenzdokumente					
Benutzerprofile					
Verwaltung von Sonderrechten					
Regelmässige Prüfung von Zugangsrechten					
Statusänderung oder Vertragsbeendigung					
Technische Umsetzung					
Verwaltung von Aufzeichnungen					
Vorgabe zur Erreichung					

Die «Zugangskontrollrichtlinie» wurde erstellt und lässt sich auf die Unternehmung anwenden.

Der Punkt gilt als erfüllt.

Für das nächste Audit ist vorzulegen:

Prüfprotokoll:	3.6. Regelmäßige Überprüfung von Zugangsrechten - Prüfprotokoll 4.0 Zugangskontrolle Sonderrechte Protokoll (Word Dokument)

d) Notfallwiederherstellungsplan

Notfallwiederherstellungsplan

	20%	40%	60%	80%	100%
Form					
History					
Zweck und Anwendungsbereich					
Annahme und Einschränkungen					
Rollen und Kontaktdaten					
Berechtigung im Krisenfall					
Verwaltung von Dokumenten					
Vorgabe zur Erreichung					

Der Notfallwiederherstellungsplan wurde erstellt im Sinne der Unternehmung. Die für den Betrieb relevanten Daten und Systeme sind bei externen Partnern als Service eingekauft und werden in der «Sicherheitsrichtlinie für Lieferanten» behandelt.

Der Punkt gilt als erfüllt.

Für das nächste Audit vorzulegen:

Erweiterung und ständige Verbesserung	5. Verwaltung von Aufzeichnungen die zu diesem Dokument erstellt wurden

e) Sicherheitsrichtlinie für Lieferanten

Sicherheitsrichtlinie für Lieferanten

	20%	40%	60%	80%	100%
Form					
History					
Zweck und Anwendungsbereich					
Beziehungen zu Lieferanten und Partnern					
Identifizierung von Risiken					
Überprüfung					
Training und Awarness					
Überwachung und Prüfung					
Änderungen bei oder Stornierung von Lieferanten-Dienstleistungen					
Entzug von Zugangsrechten / Rückgabe von Werten					
Verwaltung von Aufzeichnungen					
Anhang Sicherheitsrichtlinie für Lieferanten					
Vorgabe zur Erreichung					

Die «Sicherheitsrichtlinie für Lieferanten» mit deren Anhängen wurde erstellt und lässt sich auf die Unternehmung anwenden.

Der Punkt gilt als erfüllt.

Für das nächste Audit vorzulegen:

Training und Awareness	Planung und Durchführungstermine intern.
Überwachung und Prüfung der Lieferanten	Planung und Durchführungstermine für Lieferanten und Verträge.
Vorfallsmanagement	Alle Sicherheitsrelevanten Vorfälle mit Lieferanten müssen im Vorfallsmanagement hinterlegt werden.

f) Plan zur Risikobehandlung

Risikoeinschätzung und Risikobehandlung

	20%	40%	60%	80%	100%
Form					
History					
Zweck und Anwendungsbereich					
Methodik zu Risikoeinschätzung /-behandlung					
Identifizierung von Risiken					
Kriterien für Risikoakzeptanz					
Risikobehandlung					
Inventar der Werte					
Plan zur Risikoeinschätzung					
Risikoeinschätzung					
Plan zur Risikobewertung					
Risikobewertung					
Regelmässige Überprüfung von Risikoeinschätzung und Risikobehandlung					
Vorgabe zur Erreichung					

Plan zur Risikobehandlung wurde durch die Unternehmung erstellt und lässt sich auf die Unternehmung anwenden.

Der Punkt gilt als erfüllt.

Für das nächste Audit vorzulegen:

Termine für die Laufzeiten	Von Risiko Berichten und deren Gültigkeiten
Neue Risikoidentifizierungsdokumente	Prüfung aller neuen Bestandteile der Unternehmung vor dem Hintergrund des Datenschutzes und der Datensicherheit.
Berichte zur Risikobehandlung	Ausweisbare Verbesserungen oder Verschlechterungen der Risikobehandlung im Zeitraum der Bewertungsmatrix

Weitere Anmerkungen:

Verbesserungsvorschlag:	Bei der Risikobehandlung dürften genauere Beschreibungen helfen die Ziele zu erkennen die Bewirkt werden sollten.

g) Verfahren zum Vorfallsmanagement

Verfahren zum Vorfallsmanagement

	20%	40%	60%	80%	100%
Form					
History					
Zweck und Anwendungsbereich					
Entgegennahme und Klassifizierung von Vorfällen, Schwachstellen und Ereignissen					
Behandlungsverfahren bei Sicherheitsschwachstellen oder -ereignissen					
Behandlung geringer Vorfälle					
Behandlung erheblicher Vorfälle					
Lernen aus Vorfällen					
Sammlung von Beweisen					
Verzeichnis der Vorfälle					
Vorgabe zur Erreichung					

Das Dokument «Verfahren zum Vorfallsmanagement wurde erstellt und lässt sich auf die Unternehmung anwenden.

Der Punkt gilt als erfüllt.

Für das nächste Audit vorzulegen:

Dokument	Verzeichnis der Vorfälle

Im Einzelnen sind sämtlichen technischen Anforderungen als erfüllt zu betrachten und damit 100 % auf Basis der durchgeführten Stichproben als vollständig erfüllt anzusehen. Dort, wo es angezeigt war, wurden entsprechende Verbesserungsvorschläge festgehalten.

3. Zusammenfassung

Zählt man die Ergebnisse der rechtlichen Prüfung (84,6 %) und der technischen Prüfung (100 %) zusammen, so ergibt dies über die gesamte Prüfung gesehen ein Durchschnittsergebnis von 92,3 %.