Brandursachen-Analyse
Klarheit schaffen – Ergebnisse verwerten

Ley-Brandursachenanalyse GmbH – Gewerbestraße 9 – 56477 Rennerod

Leitlinie zur Informationssicherheit

Seitens der Geschäftsführung wird in Anbetracht des täglichen Arbeitsbedarfs in Bezug auf die Informationsbearbeitung die folgende Leitlinie zur Gewährleistung der Informationssicherheit zur Verfügung gestellt:

Inhaltsverzeichnis:

Einleitung

Als Dienstleistungsunternehmen im Bereich der Brandursachenanalyse verarbeiten wir unter anderem eine Vielzahl von personenbezogenen Daten und Informationen, welche uns regelmäßig seitens unserer Auftraggeber, aber auch durch sonstige Kenntniserlangung, zur Verfügung stehen.

Zu unseren Aufgaben und Pflichten gegenüber unseren Kunden, Vertragspartnern, Dienstleistern, Behörden und sonstigen Dritten gehört es diese Daten sicher zu verarbeiten.

Insbesondere Dateien mit einem hohen persönlichen Schutzbedarf müssen vor der unberechtigten Kenntnisnahme durch Dritte geschützt werden.

Der Sicherung der Gesamtheit der gespeicherten Informationen kommt daher im Rahmen unserer Aufgabenerfüllung eine zentrale Bedeutung zu.

Diese Leitlinie soll die Sicherheitsstrategie, die Sicherheitsorganisation und die Sicherheitsziele unseres Unternehmens darstellen.

Geltungsbereich

Diese Leitlinie gilt für das gesamte Unternehmen.

Sicherheitsziele

Während der Planung und Umsetzung unserer Geschäftsprozesse werden wir die Verfügbarkeit, Integrität und Vertraulichkeit der Daten sicherstellen.

Die konkreten Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schutzbedarf der verarbeiteten Daten stehen.

Alle Mitarbeiter des Unternehmens und die Unternehmensführung sind sich ihrer Verantwortung für die Informationssicherheit bewusst und haben diese Sicherheitsleitlinie zu unterstützen.

Sicherheitsorganisation

Zur Erreichung der Informationssicherheitsziele wurde ein IT-Sicherheitsbeauftragter, namentlich Herr Frank Schuld, seitens der Geschäftsführung bestimmt.

Verantwortlich für die Sicherheitsorganisation ist die Geschäftsführung. Der IT-Sicherheitsbeauftragte berät die Geschäftsführung bei der Planung und Umsetzung der Informationssicherheit im Unternehmen. Er berichtet in seiner Funktion anlassbezogen, mindestens jedoch einmal jährlich, unmittelbar an die Geschäftsführung.

Dem IT-Sicherheitsbeauftragten werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um eine entsprechende Datensicherheit zu gewährleisten.

Der IT-Sicherheitsbeauftragte ist frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten.

Sicherheitsmaßnahmen

Die konkreten Sicherheitsmaßnahmen sind im IT-Sicherheitskonzept auf der Basis der technischen und organisatorischenMaßnahmen i.S.d. § 9 BDSG geregelt (siehe Anlage).

Verbesserung der Sicherheit

Diese Sicherheitsleitlinie sowie das IT-Sicherheitskonzept werden regelmäßig auf ihre Aktualität und Wirksamkeit geprüft und angepasst. Die Geschäftsführung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Mitarbeiter sind angehalten, mögliche Verbesserungen oder Schwachstellen an den IT-Sicherheitsbeauftragten weiterzugeben.

Stand: 01.10.2013

Dirk Ley
(Geschäftsführer)

Ley – Brandursachenanalyse GmbH

Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG

Ley –Brandursachenanalyse GmbH
Gewerbestraße 9
56477 Rennerod

---

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- ☒ Alarmanlage (Gebäude / Serverraum)
- ☒ Videoüberwachung der Liegenschaft
- ☒ Einfriedung der Liegenschaft
- ☒ Sicherheitsschlösser
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Absicherung der Fenster
- ☒ Chipkarten-/Transponder-Schließsystem
- ☒ Manuelles Schließsystem
- ☒ Personenkontrolle bei Kundenverkehr
- ☒ Sorgfältige Auswahl von Reinigungspersonal

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- ☒ Zuordnung von Benutzerrechten
- ☒ Passwortvergabe
- ☒ Authentifikation mit Benutzername / Passwort
- ☒ Gehäuseverriegelungen
- ☒ Sperren von externen Schnittstellen (USB etc.)
- ☒ Schlüsselregelung (Schlüsselausgabe etc.)
- ☒ Sorgfältige Auswahl von Reinigungspersonal
- ☒ Einsatz einer Hardware-Firewall
- ☒ Erstellen von Benutzerprofilen
- ☒ Einsatz von Anti-Viren-Software
- ☒ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☒ Sicherheitsschlösser
- ☒ Personenkontrolle Empfang
- ☒ Einsatz einer Software-Firewall

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- ☒ Erstellen eines Berechtigungskonzepts
- ☒ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☒ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☒ ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- ☒ Brandschutzkonzept, Einhaltung der Betriebssicherheitsverordnung
- ☒ Verwaltung der Rechte durch Systemadministrator
- ☒ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☒ Sichere Aufbewahrung von Datenträgern
- ☒ Einsatz von Aktenvernichtern

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- ☒ E-Mail-Verschlüsselung
- ☒ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☒ Beim physischen Transport: sichere Transportbehälter/-verpackungen

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

☒ Protokollierung der Eingabe, Änderung und Löschung von Daten

☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

☒ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.

☒ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

☒ schriftliche Weisungen an den Auftragnehmer bzgl. des BDSG

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- ☒ Unterbrechungsfreie Spannungsversorgung (USV)
- ☒ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☒ Feuer- und Rauchmeldeanlagen
- ☒ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☒ Testen von Datenwiederherstellung
- ☒ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☒ Klimaanlage in Serverräumen
- ☒ Schutzsteckdosenleisten in Serverräumen
- ☒ Feuerlöschgeräte in Serverräumen
- ☒ Erstellen eines Backup- & Recoverykonzepts
- ☒ Serverräume nicht unter sanitären Anlagen
- ☒

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- ☒ physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☒ Erstellung eines Berechtigungskonzepts
- ☒ Logische Auftraggebertrennung (softwareseitig)
- ☒ Festlegung von Datenbankrechten