EU-Datenschutz-Grundverordnung (EU-DSGVO)

Die Vorteile einer ISO/IEC-27001-Zertifizierung durch BSI

1.378.509.261
durch Datenpannen betroffene Datensätze in 2016

58,6 %
der Vorfälle in 2016 betrafen Identitätsdiebstahl

3.776.738
Datensätze werden im Durchschnitt täglich gestohlen oder gehen verloren

1.792
Fälle von Datenschutzverstößen in 2016

Quelle: The Breach Level Index

Bei vielen Unternehmen stehen Datenschutzgesetze wie die neue europäische Datenschutz-Grundverordnung (EU-DSGVO) ganz oben auf der Agenda. Doch wie kann sich Ihr Unternehmen angemessen vorbereiten? Eine Möglichkeit ist die Zertifizierung nach ISO/IEC 27001 durch BSI.

Als international anerkannter Standard bietet die ISO/IEC 27001 ein Rahmenwerk mit bewährten Praktiken, damit Sie Ihre Informationssicherheitsrisiken, auch in Bezug auf den Schutz personenbezogener Daten, steuern können. Sie schreibt vor, dass Sie Ihre gesetzlichen Verpflichtungen, die beispielsweise aus der EU-DSGVO entstehen, nachweislich kennen und Ihnen auf geeignete Weise nachkommen. Zudem enthält die ISO/IEC 27001 Vorgaben zur Sicherheitsgestaltung und zu Rechenschaftspflichten. Zeigen Sie, dass Sie sich dem Schutz Ihrer Daten, einschließlich personenbezogener Daten, verpflichtet fühlen!

Was ist die EU-DSGVO?

Die EU-Datenschutz-Grundverordnung (EU-DSGVO), die am 25. Mai 2018 wirksam wird, ist eine neue Verordnung zum Schutz personenbezogener Daten. Sie soll die Datenschutzgesetzgebung im europäischen Binnenmarkt harmonisieren und Einzelpersonen die Kontrolle über ihre Daten zurückgeben. Sie wird internationale Geschäftsbeziehungen fördern und Verbrauchern die Gewissheit geben, dass ihre Daten sicher sind.

Wer ist betroffen?

- Sowohl Verantwortliche als auch Auftragsdatenverarbeiter von personenbezogenen Daten
- Alle EU-Mitgliedsstaaten sowie jede Organisation, die auf dem europäischen Markt tätig ist und Daten von europäischen Datensubjekten besitzt

Wie fügt sich die ISO/IEC 27001 in die EU-DSGVO ein?

Risikoabschätzung

In den neuen Verordnungen sind hohe Geldstrafen vorgesehen, die sich schmerzlich auf die Finanzen Ihrer Organisation auswirken können (bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes der Muttergesellschaft). Die ISO/IEC 27001 verlangt eine Risikoabschätzung Ihrer Informationswerte, worunter natürlich auch das gestiegene Risiko in Bezug auf personenbezogene Daten und die möglichen finanziellen Auswirkungen fallen.

Compliance

Das neue Gesetz wird am 25. Mai 2018 wirksam; bis dahin müssen Sie Ihre Pflichten kennen. Die ISO/IEC 27001 schreibt vor, dass Sie relevante gesetzliche oder vertragliche Anforderungen auflisten und ihre Einhaltung sicherstellen.

Klassifizierung von Daten

Bei der Verarbeitung von personenbezogenen Daten muss deren Schutz sichergestellt sein. Für die Zertifizierung nach ISO/IEC 27001 müssen Organisationen die Daten, die sie empfangen, auf eine Weise schützen, die der Bedeutung der Daten für die Organisation entspricht.

bsi.

...making excellence a habit.™

Anzeige von Datenpannen

Unternehmen müssen, sobald ihnen eine Datenpanne bekannt wird, innerhalb von 72 Stunden die Aufsichtsbehörden informieren. Die ISO/IEC 27001 schreibt einen Prozess zum Umgang mit Informationssicherheitsvorfällen vor, bei dem Informationssicherheitsereignisse so schnell wie möglich über geeignete Managementkanäle gemeldet werden.

Zusammenarbeit mit Behörden

Nach der EU-DSGVO müssen Organisationen mit Behörden, etwa den für den Daten- und Persönlichkeitsschutz zuständigen Aufsichtsbehörden, zusammenarbeiten. Die ISO/IEC 27001 verlangt, „geeignete Kontakte zu relevanten Behörden" zu pflegen.

Management von organisationseigenen Werten

Gemäß EU-DSGVO müssen Sie nachvollziehen können, welche personenbezogenen Daten Sie sammeln, wie Sie in den Besitz der Daten gelangt sind, wo die Daten gespeichert sind, wie lange die Daten gespeichert werden und wer auf die Daten zugreifen kann. Im Rahmen der Anforderungen der ISO/IEC 27001 bestimmen Sie organisationseigene Werte (Assets) und definieren die Verantwortung für deren angemessenen Schutz. Sie müssen ein Inventar der Assets erstellen, den Eigentümer der Assets bestimmen, Regeln für den zulässigen Gebrauch der Assets aufstellen und bestimmen, was am Ende ihres Lebenszyklus mit den Assets passiert.

Eingebauter Datenschutz

Eine weitere Forderung der EU-DSGVO ist, dass der Datenschutz durch die Technikgestaltung sichergestellt ist. Die ISO/IEC 27001 sieht vor, dass bereits bei der Entwicklung von Informationssystemen für den gesamten Lebenszyklus die Informationssicherheit berücksichtigt und umgesetzt wird.

Lieferantenbeziehungen

Die EU-DSGVO gilt auch für Lieferanten, die personenbezogene Daten im Auftrag anderer verarbeiten. Die Kontrollen und Beschränkungen müssen hierbei vertraglich geregelt sein. Betroffen sind Internet- und Cloudanbieter sowie ausgegliederte Rechenzentren. Die ISO/IEC 27001 verlangt von Organisationen, die für Lieferanten zugänglichen organisationseigenen Werte zu schützen, und die Dienstleistungserbringung durch Lieferanten in Bezug auf Informationssicherheitsanforderungen zu überwachen.

Dokumentation

Verantwortliche im Sinne der EU-DSGVO müssen u. a. dokumentieren, zu welchem Zweck Daten gesammelt und verarbeitet werden und welche „Kategorien" von betroffenen Personen und von personenbezogenen Daten es gibt. Die Dokumentationspflichten im Rahmen der ISO/IEC 27001 richten sich nach der Komplexität der Prozesse und dem Zusammenwirken dieser Prozesse.

Warum BSI?

Im Jahr 1995 schufen wir mit der BS 7799 nicht nur den ersten Standard im Bereich der Informationssicherheit, sondern auch den Vorläufer der ISO/IEC 27001. Seitdem sind wir federführend an der Entwicklung von Informationssicherheitsstandards beteiligt und stellen sicher, dass auch aktuelle Themen wie Cyber- und Cloudsicherheit berücksichtigt werden. Wer also wäre besser geeignet, Sie bei der Umsetzung von Datenschutzvorgaben zu unterstützen, als wir?

Wird irgendetwas nicht von der ISO/IEC 27001 abgedeckt?

Die ISO/IEC 27001 bietet einen guten Rahmen, der Ihre Verpflichtung zu Informationssicherheit und Datenschutz zeigt. Viele der Anforderungen der EU-DSGVO werden von ihr abgedeckt. Sie sollten jedoch auch folgende Aspekte bedenken:

- **Schulung und Sensibilisierung**
  Stellen Sie sicher, dass Ihr Management und die wichtigsten Interessenträger die geänderten gesetzlichen Anforderungen kennen. Gegebenenfalls müssen Sie ihnen die möglichen Auswirkungen von Verstößen aufzeigen und sie eingehender schulen.

  Falls Sie selbst Ihr Wissen erweitern möchten, können Sie sich in einem unserer Kurse zum Datenschutz weiterbilden, beispielsweise in unserem Grundlagenkurs zur EU-Datenschutz-Grundverordnung.

- **Datenschutzbeauftragter**
  Manche Maßnahmen, etwa die großangelegte Überwachung von Einzelpersonen oder die Verarbeitung von Daten bestimmter Kategorien, machen die Ernennung eines Datenschutzbeauftragten erforderlich. Selbst wenn es nicht zwingend nötig ist, einen Datenschutzbeauftragten zu ernennen, macht ein zentraler Ansprechpartner mit Fachwissen im Bereich Informationssicherheit und Kenntnis von Datenschutzgesetzen immer einen guten Eindruck.

- **Überprüfung Ihrer Verfahren**
  Vergewissern Sie sich, dass alle Rechte von betroffenen Personen durch Ihre Verfahren abgedeckt sind. Personenbezogene Daten müssen beispielsweise sachlich richtig sein, dürfen nur zu dem Zweck verwendet werden, zu dem sie auch gesammelt wurden, und dürfen nicht länger gespeichert werden als nötig. Sie müssen außerdem sicherstellen können, dass Sie auf Begehren der betroffenen Person Auskunft über die gespeicherten Daten geben oder sie löschen können.

- **Systemoptimierung**
  Wenn Sie Informationen in der Public Cloud speichern oder verarbeiten, ist die ISO/IEC 27018 möglicherweise von Interesse für Sie. Ausgehend von einem ISO/IEC-27001-konformen System verpflichtet die ISO/IEC 27018 Organisationen dazu, Angaben über bestimmbare Personen zu schützen.

- **Erweiterung des Control-Set**
  Die ISO 27001 erlaubt neben dem Anhang A weitere Quellen zur Maßnahmenplanung hinzuzuziehen. Wir empfehlen:
  – In Verbindung mit dem IT-Sicherheitskatalog für Energienetzbetreiber das erweiterte Control-Set ISO 27019
  – Für die Anforderungen aus der EU-Datenschutz-Grundverordnung das erweiterte Control-Set basierend auf der Normserie ISO29100 ff.

Sie wollen komplett auf Nummer sicher gehen?
Der britische Standard BS 10012 bietet ein Rahmenwerk bewährter Praktiken in Bezug auf Managementsysteme für personenbezogene Daten. Die Anforderungen der EU-DSGVO wurden in einer kürzlich erfolgten Überarbeitung aufgenommen. Die BS 10012 ist möglicherweise eine hilfreiche Zusatzlektüre oder sogar eine sinnvolle Ergänzung Ihres bestehenden Managementsystems und wird von BSI als eigenständiges Managementsystem zertifiziert.

Weitere Informationen
Telefon: **+49 69 2222 8 9200**
Website: **bsigroup.de**