Verbund Innovativer Automobilzulieferer

News

Juli 2016

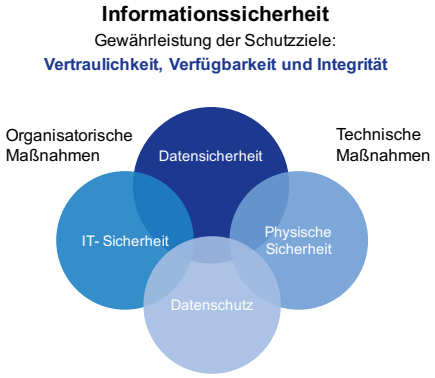
Abgrenzung zwischen IT-Sicherheit, Datensicherheit, Datenschutz & Informationssicherheit

Informationssicherheit – Informationssicherheitsmanagementsystem (ISMS)

Datenschutzbeauftragter – Aufgaben und Position

Abgrenzung zwischen IT-Sicherheit, Datensicherheit, Datenschutz & Informationssicherheit

Datenschutz, Datensicherheit, Informationssicherheit oder IT-Sicherheit: Viele Begriffe, die sich unterscheiden und doch oft falsch verwendet werden. Nachfolgend sollen die Unterschiede erklärt und auf klassische Schutzziele hingewiesen werden.



Begriffe der Informationsssicherheit

Datenschutz

Bei dem Datenschutz geht es um den Schutz der Privatsphäre eines jeden Menschen. Datenschutz schützt nicht die Daten, sondern die Personen. Er garantiert jedem Bürger ein Recht darauf selbst über seine Daten zu bestimmen und schützt ihn vor deren missbräuchlichen Verwendung. Die Verarbeitung personenbezogener Daten ist in verschiedenen Gesetzen geregelt, hauptsächlich gelten aber die Regelungen des Bundesdatenschutzgesetztes (BDSG).

Die Regelungen des BDSG betreffen alle Unternehmen (nicht öffentliche Stellen) und öffentliche Stellen, die Daten unter Nutzung von EDV verarbeiten. Als eine Forderung schreibt das BDSG z.B. die Benennung eines Datenschutzbeauftragten (DSB) für alle Unternehmen vor, in denen mehr als neun Personen mit personenbezogenen Daten (bspw. auch Vorname und Nachname in einer Excel-Datei) arbeiten. Das bedeutet, dass im Grunde alle Unternehmen mit mehr als neun-PC-Arbeitsplätzen einen DSB bestellen müssen.

Datensicherheit

Im Unterschied zum Datenschutz befasst sich die Datensicherheit mit dem Schutz aller Daten, unabhängig davon ob diese personenbezogen sind oder nicht. Unter die Datensicherheit fallen damit zum Beispiel auch Unternehmensdaten (z.B. Konstruktionsdaten).

Bei der Datensicherheit sollen durch das Treffen geeigneter Maßnahmen Risiken minimiert, ausgeschlossen oder abgesichert werden. Die drei Schutzziele für Daten Vertraulichkeit, Verfügbarkeit und Integrität, die im Folgenden noch genauer beschrieben werden, sollen dadurch gewährleistet werden.

Die Datensicherheit ist in Bezug auf personenbezogene Daten ebenfalls ein Teil des BDSG, welches die Gewährleistung eines angemessenen Schutzniveaus vorschreibt (§9 BDSG „Technische und organisatorische Maßnahmen“).

IT-Sicherheit

Die Begriffe IT-Sicherheit und Informationssicherheit werden oft fälschlicherweise gleichgesetzt. Die IT-Sicherheit bezieht sich jedoch ausschließlich auf elektronisch gespeicherte Informationen und IT-Systeme während sich die Informationssicherheit mit allen Informationen befasst.

Informationssicherheit

Der Begriff der Informationssicherheit beinhaltet die drei vorgenannten Begriffe Datenschutz, Datensicherheit und IT-Sicherheit – sie ist aber noch deutlich weiter zu fassen. Bei der Informationssicherheit geht es um alle Informationen, die in welche Form sie auch immer vorliegen. Die Informationssicherheit betrachtet daher auch Gegenstände wie beispielsweise Prototypen. Aus diesem Grund ist auch die physische Sicherheit ein Teil der Informationssicherheit.

Schutzziele der Informationssicherheit

Die Informationssicherheit soll die Gewährleistung der 3 Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit für alle Informationen sicherstellen.

Die Gewichtung und Einstufung von Informationen und somit die Schutzziele muss jedes Unternehmen einzelfallabhängig vornehmen. Um die Schutzziele zu erreichen, müssen technische und organisatorische Maßnahmen umgesetzt werden.

Informationssicherheitsmanagementsystem

Die Schutzziele der Informationssicherheit können z.B. durch ein Informationssicherheitsmanagementsystem (ISMS) identifiziert und realisiert werden. Der Aufbau eines solchen Systems kann sowohl nach der DIN ISO 27001 als auch nach dem BSI-Grundschutz durchgeführt werden. Beide Standards verwenden die gleichen Kernelemente, beinhalten aber eine unterschiedliche Vorgehensweise. Während der BSI-Grundschutz einen sehr IT-lastigen Ansatz verfolgt, ist die Herangehensweise der DIN ISO 27001 eher organisatorisch nach dem Plan-Do-Check-Act-System, welches bereits aus anderen Managementsystemen bekannt ist. Der BSI-Grundschutz ist ein rein deutscher Standard, wohingegen die DIN ISO 27001 eine international anerkannte Norm ist. Zudem ist die Norm in der High Level Struktur verfasst, wie sie zukünftig auch bei den anderen Normen für Managementsysteme verwendet wird. Dadurch ist das ISMS ähnlich aufgebaut wie die bereits bekannten Managementsysteme und kann in bereits bestehende Systeme integriert werden.

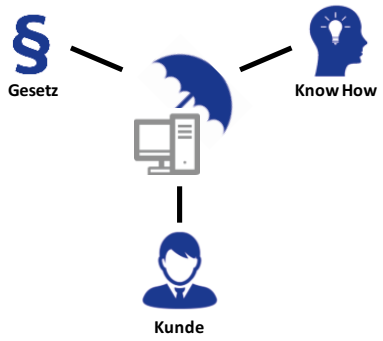
Im Gegensatz zum Datenschutz, der durch das Bundesdatenschutzgesetz verpflichtend einzuhalten ist und dessen Anforderungen zwingend zu erfüllen sind, wird die Informationssicherheit bzw. ein ISMS aus eigenem Interesse des Unternehmens betrieben. Aufgrund von Kundenanforderungen (beispielsweise durch ISMS-Audits von VW) steigt die Notwendigkeit eines Informationssicherheitsmanagementsystems jedoch stark an, so dass dieses häufig nicht mehr nur aus eigenem Interesse, sondern aufgrund von Forderungen durch den Kunden eingeführt wird/ werden muss.

Weitere detaillierte Informationen zum Datenschutz und zum Informationssicherheitsmanagementsystem finden Sie auf den folgenden Seiten. Gerne können Sie uns bei Fragen zu diesem Thema auch persönlich ansprechen.

Informationssicherheit – Informationssicherheitsmanagementsystem (ISMS)

Die Einführung eines ISMS kann verschiedene Gründe haben.

Die drei häufigsten Gründe für die Einführung eines ISMS stellen zugleich auch die drei Ursprünge dar, aus denen Anforderungen an das ISMS resultieren können.



Ursprünge und Gründe für ein ISMS

1. Gesetzliche Vorgaben

a) Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz schreibt vor, dass technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten umgesetzt werden müssen. Auch die Umsetzung dieser Forderung kann einen Teilbereich des ISMS abdecken, bzw. eine Grundlage hierfür sein.

b) IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz trat im Juli 2015 in Kraft und beschäftigt sich mit der Erhöhung der Sicherheit informationstechnischer Systeme. Aus dem Erlass dieses Gesetzes ergeben sich Änderungen in anderen Gesetzen, wie z.B. im Telemediengesetz. Insbesondere ändert es das BSI-Gesetz, dass nun auch die Sicherheit Kritischer Infrastrukturen regelt. Demnach müssen Betreiber Kritischer Infrastrukturen (diese sind in einer Verordnung genauer definiert) „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse“ treffen und diese alle 2 Jahre in „geeigneter Weise“ nachweisen. Die Energiewirtschaft regelt dies voraussichtlich z.B. über einen Sicherheitskatalog, der die verpflichtende Einführung der DIN ISO 27001 festlegt.

2. Externe Parteien (insbesondere Kundenanforderungen)

Immer häufiger realisieren Kunden, dass sehr viel ihres Know-Hows bei den Zulieferern liegt und definieren daher eigene Anforderungen in der Informationssicherheit, die durch die Zulieferer eingehalten werden müssen. Für die Automobilindustrie sind diese Anforderungen bspw. in einem VDA-Fragenkatalog beschrieben, der jedoch fast deckungsgleich mit den Inhalten der DIN ISO 27001 ist. Zudem geben die OEMs noch eigene Sicherheitsrichtlinien heraus. Diese beschreiben häufig zusätzliche Anforderungen in den Bereichen physische Sicherheit und Prototypenschutz.

Weitere Anforderungen können außerdem von anderen externen Parteien, wie z.B. Versicherungen, Wirtschaftsprüfern o.ä. kommen.

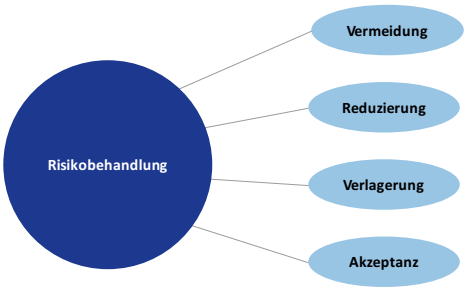
3. Eigeninteresse (Know-How-Schutz)

Selbstverständlich kann ein ISMS auch aus eigenem Antrieb eingeführt werden. Insbesondere Unternehmen, die eigenes Know-How entsprechend schützen wollen / müssen, betreiben häufig schon einige Jahre ein ISMS – auch wenn dies meist nicht als ein solches angesehen wird.

Abhängig von den verschiedenen Gründen zum Betrieb eines ISMS ergibt sich auch eine unterschiedlich starke Sicherung der einzelnen Informationen, was jeweils abhängig von der Einstufung des Schutzbedarfes der Informationen durch das Unternehmen ist. Nicht immer bedeutet ein ISMS aber, dass unbedingt eine Zertifizierung des Informationsmanagementsystems z.B. nach DIN ISO 27001 durchgeführt werden muss. Ein Informationsmanagementsystem kann – wie bspw. auch ein QM- oder Energiemanagementsystem – auch eigenständig und ohne Zertifizierung wirksam durchgeführt werden. Wird jedoch eine Zertifizierung angestrebt, sind zwingend die Anforderungen der Zertifizierungsstandards (DIN ISO 27001 oder BSI-Grundschutz) zu erfüllen.

Kernelement der DIN ISO 27001 ist die Struktur- und Risikoanalyse / -behandlung. Hierbei werden alle Werte des Unternehmens aufgenommen, nach Ihrem Schutzbedarf z.B. in den Schutzzielen Vertraulichkeit, Verfügbarkeit und Integrität bewertet und eine entsprechende Risikoanalyse durchgeführt.

Werden Risiken entdeckt, müssen diese entsprechend behandelt werden.



Möglichkeiten der Risikobehandlung

Aus der Risikobehandlung ergeben sich dann entsprechende Maßnahmen, wie z.B. die Reduzierung des Ausfalls von Internet und E-Mail durch Inbetriebnahme einer zweiten (kleineren) Leitung bei einem zweiten Anbieter. Nach der Risikobehandlung wird die Risikoanalyse von neuem bewertet, so dass in einem kontinuierlichen Prozess die größten Risiken verringert werden.

Wenn Sie Interesse an oder Fragen zur Informationssicherheit oder einem ISMS haben, sprechen Sie uns gerne an.

Vertraulichkeit *bedeutet, sicherzustellen, dass nur befugte Personen Informationen erlangen oder einsehen können.*

Integrität *bedeutet, dass Daten / Systeme korrekt, unverändert und verlässlich sind. Die Integrität kann z.B. bei einer absichtlichen Verfälschung von Daten, aber auch bei fehlerhaft arbeitender Soft- oder Hardware gefährdet sein.*

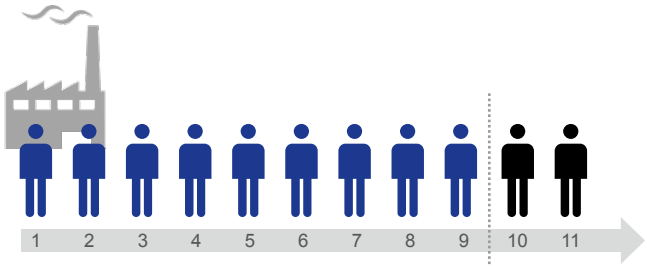
Verfügbarkeit *bedeutet, dass Daten und IT-Systeme zur Verfügung stehen und von autorisierten Personen genutzt werden können, wenn sie benötigt werden.*

Wann benötige ich einen Datenschutzbeauftragten, welche Aufgaben übernimmt dieser im Unternehmen und wer kann diese Position übernehmen?

Es herrscht häufig noch eine große Ungewissheit, wann ein Datenschutzbeauftragter überhaupt benötigt wird und welche Aufgaben dieser dann im betrieblichen Alltag übernehmen soll. Auch die Kriterien dafür, wer diesen Posten einnehmen kann, sind nicht durchgängig bekannt. All diese Fragestellungen sollen im weiteren Verlauf anschaulich geklärt werden.

Notwendigkeit des Datenschutzbeauftragten

Ihr Unternehmen beschäftigt mehr als neun Personen, welche mittels automatisierten Verfahren personenbezogene Daten verarbeiten bzw. mehr als 19 Personen, die personenbezogene Daten ohne automatisierte Verfahren verarbeiten? Dann benötigen Sie gemäß § 4f Bundesdatenschutzgesetz einen Datenschutzbeauftragten. Dabei ist es unwesentlich, welche Art automatisierten Verfahrens sie verwenden (z.B. Office, ERP, CAQ etc.).



Bemessungsgrenze bei der Anwendung automatisierter Verfahren

Personenbezogene Daten (pbD) sind Einzelangaben zu persönlichen und sachlichen Verhältnissen, wie beispielsweise der Vor- und Nachname, Kontaktdaten, Sozialversicherungsnummer, Krankendaten etc. Somit sind pbD (bspw. der Mitarbeiter) in jedem Unternehmen zu finden, da diese z.B. in Dateisignaturen, in Excel-Listen, bei Lager- oder Reklamationsbuchungen, Zeiterfassung usw. für den Geschäftsbetrieb verwendet werden. Vereinfacht kann also gesagt werden, wenn Sie mehr als 9 Personen beschäftigen, die an einem PC arbeiten, benötigen Sie einen Datenschutzbeauftragten.

Aufgaben des Datenschutzbeauftragten

Der Datenschutzbeauftragte übt seine Tätigkeit weisungsfrei aus und ist der Unternehmensleitung dabei direkt unterstellt. Im Rahmen seiner Tätigkeit ist der Beauftragte zur Verschwiegenheit verpflichtet und besitzt während und nach seiner Bestellung einen besonderen Kündigungsschutz. Eine Kündigung ohne wichtigen Grund ist somit unzulässig.

Zu den Aufgaben des Datenschutzbeauftragten gehört unter anderem die Überprüfung der Einhaltung der datenschutzrechtlichen Bestimmungen durch regelmäßige Hinterfragung von Abläufen im Unternehmen, sowie das Schulen und Sensibilisieren der Mitarbeiter hinsichtlich der Anforderungen des Datenschutzes. Dabei ist es gerade wichtig die Personengruppen zu sensibilisieren, welche im betrieblichen Alltag mit den besonders schützenswerten personenbezogenen Daten in Kontakt kommen, wie bspw. die Personalabteilung.

Daneben ist es notwendig bei neu einzuführenden Systemen, welche automatisiert besondere personenbezogene Daten verarbeiten oder die Leistung und Persönlichkeit eines Mitarbeiters bewerten, eine Vorabkontrolle durchzuführen. Im Rahmen dieser Überwachung überprüft der Datenschutzbeauftragte in wie weit eine Verarbeitung der besonderen personenbezogenen Daten überhaupt notwendig ist und welche Risiken eventuell bei einer Auswertung entstehen können. Er wahrt somit die Rechte der betroffenen Personengruppen im Unternehmen.

Ergänzend dazu überprüft und optimiert der Beauftrage die technischen und organisatorischen Maßnahmen (TOM). Diese dienen dazu, ein gewisses Sicherheits- und Schutzniveau herzustellen. Somit soll vermieden werden, dass unberechtigte Dritte Zugriff auf sensible Daten der Mitarbeiter bekommen. Hier ist wieder die Überschneidung zur Informationssicherheit zu finden.

Um eine Übersicht über die Systeme zu bekommen, welche personenbezogene Daten im Unternehmen verarbeiten, führt der benannte Datenschutzbeauftragte ein Verfahrensverzeichnis. Im Detail führt dieses Verzeichnis auf, welche personenbezogenen Daten zu welchem Zweck im Unternehmen verarbeitet werden. Das Bundesdatenschutzgesetz beschreibt hier konkrete Vorgaben welche Angaben gemacht werden müssen.

Bestellung des Datenschutzbeauftragten

Die Position des Datenschutzbeauftragten kann durch eine interne Person sowie durch eine externe Person besetzt werden.

Interne Besetzung

Hier gilt es zu beachten, dass diejenige Person unabhängig und neutral in ihrer Aufgabenausführung handeln muss. Ein Datenschutzbeauftragter, welcher beispielsweise zusätzlich Führungskraft einer Fachabteilung ist, welche unentwegt mit personenbezogenen Daten arbeitet, ist im Sinne des Bundesdatenschutzgesetzes nicht rechtmäßig. Dazu gehört bspw. bei kleineren Organisationen auch der IT-Leiter. Daneben muss die Person die notwendige Fachkunde besitzen um in der Anwendung des Bundesdatenschutzgesetztes sicher handeln zu können.

Externe Besetzung

Für eine externe Besetzung spricht die Tatsache, dass der externe Dritte einen neutraleren Blick auf die internen Abläufe legen kann. Zusätzlich bindet die externe Fachkraft keine internen Ressourcen, was dem Unternehmen wiederum erlaubt sich auf seine Kernkompetenz zu konzentrieren.

Gerne geben wir Ihnen auch persönlich im Detail weitere Auskünfte zum Thema Datenschutz im Unternehmen.

Impressum

Verbund Innovativer Automobilzulieferer

Ausgabe Juli 2016
Auflage 1200 Exemplare
Herausgeber VIA Consult GmbH & Co. KG, Martinstraße 25, 57462 Olpe
E-Mail: info@v-i-a.de · Telefon: 02761/8375-0
Satz & Druck FREY Print + Media GmbH, Attendorn