



Firmenname	ACCEL GmbH
Ansprechpartner	Hr. Bernhard Kurpicz
Adresse	Zum Pier 73-75, 44536 Lünen
Telefon	0231 39995 0
Datum	16.06.2009

Beitrag der ACCEL GmbH zum Wettbewerb „IT-Sicherheitspreis NRW 2009

Toolgestützte Selbstbewertung des Datenschutzstandards eines Unternehmens mittels ACCEL.DPB (Data Privacy Benchmark)

Jeder Unternehmer weiß, dass das Thema Datenschutz eine essentielle Anforderung an die eigene Organisation ist. Dennoch herrscht teilweise eine große Unsicherheit. Viele fragen sich: „Was bedeutet Datenschutz für mein Unternehmen?“. Diese Frage führt zu weiteren Unterfragen:

- Immer wieder liest man Formulierungen wie „Unser Unternehmen erfüllt den Branchenstandard im Datenschutz.“ Was bedeutet „Branchenstandard“? Gibt es einen für IT im Mittelstand?
- Ab wann benötigt mein Unternehmen einen Datenschutzbeauftragten?
- Welche Position im Unternehmen darf der Datenschutzbeauftragte haben oder nicht haben? Habe ich diese Position richtig besetzt
- Welche Kunden- und Mitarbeiterdaten müssen in welcher Form behandelt werden? Welche Daten erfordern ggf. eine gesonderte sicherere Datenhaltung?
- Welche Datenschutzrichtlinien schreibt die EU für mein Unternehmen vor? An was muss ich mich halten, wenn ich Kundendaten aus Frankreich, Irland oder Ungarn speichere?
- Wie prüfe ich, ob die Verarbeitung von Daten in meinem Unternehmen konform zum Bundesdatenschutzgesetz (BDSG) ist?
- ...

Wie vergleichbar ist Datenschutz?

- Auf nationaler Ebene gelten die Vorgaben des BDSG.
- Darüber hinaus gibt es zahllose individuelle und Branchenstandards, z.B. TÜV-SÜD „s@fer-website“, EU-Richtlinien für den kommerziellen Mail-Versand, etc., die ggf. für das eigene Unternehmen Relevanz haben.
- Für einzelne Branche gehört es darüber hinaus zum Datenschutz, branchenübliche Verschlüsselungsstandards einzuführen, deren Anwendung nicht in Gesetzestexten zu finden ist (etwa bei Banken oder Behörden).

Basierend auf diesen Eckdaten ist es nicht mehr weit zu der Idee, einen Fragenkatalog für die Grundlagen des Datenschutzes zu erstellen, der es Unternehmen und Organisationen ermöglicht, die eigenen Datenschutzerfordernungen individuell zu bewerten und so mit vergleichsweise geringem finanziellen und zeitlichen Aufwand die eigenen Notwendigkeiten zu analysieren. Relevante Standards werden zu einem umfassenden Fragenkatalog vereint werden, der alle Belange des Unternehmens oder einer Branche abdeckt. Die individuelle Relevanz einzelner Unterthemen wird nach Auswahlkriterien selektiert.

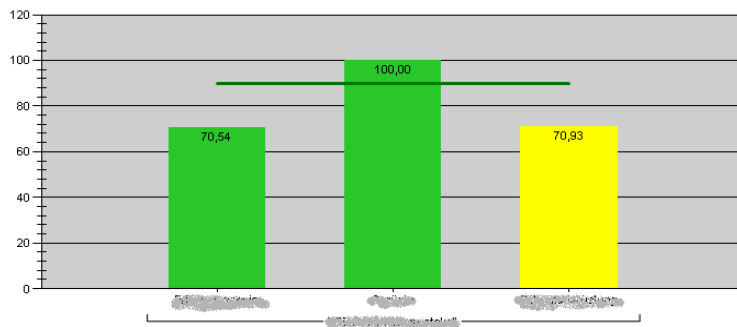
- Grundlage des Fragenkatalogs bildet das Bundesdatenschutzgesetz, da dies die engmaschigsten Richtlinien zum Datenschutz bietet, die momentan in Deutschland Anwendung finden und das auch im internationalen Vergleich führend ist. Für in Deutschland ansässige Unternehmen ist dies auch für Aktivitäten im Ausland die beste Grundlage.
- Eventuell vorhandene Unternehmens- oder Gruppenstandards (oder auch Branchenstandards) werden bei Bedarf mit einbezogen werden und bereichern den Fragenkatalog an.
- Kriterien zur Auswahl der relevanten Faktoren sind beispielsweise:
 - Wie groß ist das Unternehmen?
 - In welcher Branche ist das Unternehmen tätig?
 - Hat das Unternehmen Umgang mit vertraulichen Daten?
 - ...

Ein solcher Fragenkatalog kann schließlich auf Basis der Softwarelösung ACCEL.DPB (Data Privacy Benchmark) datentechnisch verarbeitet werden. ACCEL.DPB ermöglicht auf Grundlage der SASQIA-Technologie die Umwandlung von Regelwerken in feingranulare Fragenkataloge, die zu einem Selbstaudit verwendet werden können. Durch die feine Strukturierung der Fragenkataloge können die Fragen eindeutig beantwortet werden und lassen keinen Raum für Interpretationen, die andernfalls das Ergebnis verfälschen könnten. Das Prinzip dieser Fragenkataloge wurde bereits bei der Lieferantenbewertung und bei der Selbstbewertung hinsichtlich diverser Qualitätsstandards erfolgreich umgesetzt. Jetzt ist die Selbstbewertung der Compliance bezüglich des Datenschutzes ein weiterer Schritt, der gerade dem mittelständischen Unternehmen einen deutlichen Mehrwert bietet. Das Prinzip von ACCEL.DPB hier einmal im Überblick:

- Bestehende Regelwerke werden in Fragenkataloge umgewandelt.
- Zur Beantwortung der Fragenkataloge gibt es vorgegebene Auswahlmöglichkeiten.
- Die für die Rahmendaten des Unternehmens passenden Standards werden ausgewählt.
- Aufgrund der feinen Granularität der Fragenkataloge ist eine eindeutige Beantwortung der Fragen gewährleistet.
- Dies resultiert in einer eindeutigen Bestimmung der Compliance zu den Datenschutzrichtlinien.

Auswertung / Compliance

- Die Performance gegen den vorgegebenen Standard kann anschließend auch grafisch ausgewertet werden. Hier sind auch abweichende Bewertungen möglich, etwa wenn sich verschiedene Fachbereiche der Selbstbewertung unterzogen haben und Kriterien nur in einzelnen Teilen der Organisation erfüllt sind.
- Die Analyse des ausgefüllten Fragenkatalogs zeigt auf, wo die Organisation dem Standard entspricht, wo gute Ansätze vorhanden sind oder wo eventueller Handlungsbedarf besteht.



Vergleichbarkeit der Ergebnisse!

- Aufgrund der einheitlichen Fragenkataloge werden die Ergebnisse vergleichbar. Der Selbsteinschätzung von Unternehmen bezüglich ihrer Datenschutz-Compliance wird ihre Subjektivität genommen und durch eindeutige Bewertungen ersetzt.
- Einheitliche Validierung der Compliance zu den gesetzlichen und unternehmensinternen Anforderungen an den Datenschutz ermöglicht auch eine neutrale Einschätzung der Positionierung gegenüber dem Wettbewerb.
- Die standardisierte Datenbasis ist auf Grundlage des legalen Rahmenwerks erstellt worden.
- Eine qualifizierte Selbstbewertung bietet Unternehmen Rechtssicherheit bezüglich des Datenschutzes.

Technologie

- ACCEL.DPB ist ein webbasiertes Tool. Für den Einsatz innerhalb der eigenen Infrastruktur genügt ein PC mit einem gängigen Browser.

Fazit

- Datenschutz in der IT ist für mittelständische Unternehmen ein Feld, das Regelungen unterliegt, die nicht unbedingt auf den ersten Blick zu durchschauen sind.
- Selbstbewertung auf Grundlage der Bundesdatenschutzgesetzes und weiterer Industriestandards bietet eine Orientierung bezüglich der Datenschutz-Compliance der eigenen Organisation und liefert genauen Aufschluss darüber, in welchen Bereichen Handlungsbedarf besteht, bevor ein externer Auditor oder gar ein Kunde dies feststellt.
- Eigene Datenschutzrichtlinien können zusätzlich eingebunden werden um etwa interne Audits mit den einzelnen Fachbereichen durchzuführen.
- Das Prinzip der toolgebundenen Selbstbewertung gegen nationale und internationale Standards sowie interne Richtlinien ist aus anderen Softwareprodukten der ACCEL bereits bekannt und von namhaften Kunden in der Praxis für gut befunden worden. Durch die Einbindung der Bewertung von Datenschutz-Richtlinien wird ein Themengebiet hinzugewonnen, in dem vielen Unternehmen ein klares Regelwerk für die Ausrichtung ihrer IT heute noch fehlt.