

Datenschutz im Unternehmen

Auszug Risikoanalyse

erste Empfehlungen zur Umsetzung des Datenschutzes

erstellt für die

**Muster GmbH
Muster-Info-Straße 13
12345 Musterhausen**

Warum Datenschutz?

- 1. Laut Bundesdatenschutzgesetz** sind Unternehmen verpflichtet, einen Datenschutzbeauftragten zu bestellen, wenn mehr als 9 Personen mit personenbezogenen Daten (Mitarbeiter, Kunden, Lieferanten) in elektronischer Form umgehen. Dazu zählen alle Mitarbeiterinnen und Mitarbeiter, egal in welchem Beschäftigungsstatus, Geschäftsführer einer GmbH, wenn sie nicht beherrschende Gesellschafter sind, aber auch Aushilfskräfte, Auszubildende, Studenten usw.. Diese Verpflichtung besteht europaweit 1999, in der Bundesrepublik Deutschland gibt es das Bundesdatenschutzgesetz seit 1989, in der europäisierten Form seit 2003. Seither bestehen auch die Verpflichtungen für die Unternehmen. Bei Zuwiderhandlungen drohen Geldbußen bis 25.000 €, wenn mit dem Willen der Bereicherung entsprechende Verletzungen des Gesetzes begangen werden sogar bis 250.000€.
- 2. Die Kunden wollen Datenschutz**
Immer mehr Kunden erwarten auch z.B. von ihrem Energieversorger, dass ihre Daten besonders sorgfältig behandelt werden. Sie haben das gesetzlich verbriefte Recht, zu erfahren, welche Daten über sie gespeichert sind, wie diese Daten ins Unternehmen gekommen sind und an wen sie weitergegeben wurden und werden.
- 3. Datenschutz hindert nicht**, sondern vereinfacht im Gegenteil viele Geschäftsprozesse, aber nur, wenn er von Experten richtig umgesetzt wird. Weil bei gut gemachtem Datenschutz erstmals im Unternehmen die Verwaltungsgeschäftsprozesse analysiert werden (es gilt, den Weg der Daten aufzuzeichnen), kann mit der Einführung des Datenschutzes erstmals die Chance zur Optimierung dieser Prozesse genutzt werden.
- 4. Sicherheit durch Qualifikation**
Die EUWIS GmbH schult interne Datenschutzexperten mit IHK-Zertifikat. Durch die Praxisübungen erhalten Sie die notwendige Qualifikation für die Umsetzung in der Praxis.
- 5. Integraler Bestandteil des Qualitätsmanagements**
Vor allem beim Audit in Unternehmen mit QMS verlangen die Auditoren immer häufiger den Nachweis, dass Datenschutz und IT-Sicherheit auch tatsächlich gelebt werden und nicht nur auf dem Papier vorhanden sind.
- 6. Geschäftsführer von GmbHs haften persönlich** bei Verstößen im Rahmen der Durchgriffshaftung
- 7. Imageförderung**
Vorhandener Datenschutz kann zur Imageförderung eingesetzt werden. Für Ihre Kunden ist es ein echter Vertrauensbonus, wenn sie merken, dass ihre persönlichen Daten sehr sorgsam behandelt werden.
- 8. In der Wirtschaft werden immer häufiger Aufträge vom Vorhandensein von einem schlüssigen IT-Sicherheitskonzept und von Datenschutz abhängig gemacht.**

Team-Datenschutz: So einfach kann Datenschutz sein

Team Datenschutz ist ein Kompetenznetzwerk von Datenschutzbeauftragten, das deutschlandweit tätig ist.

Vielfältige Fachkompetenz: Was uns von andern unterscheidet, ist unsere äußerst vielfältige Fachkompetenz, denn jeder von uns führt ein Unternehmen oder ist freiberuflich tätig und betreibt Datenschutz als ein zentrales Standbein.

Qualifikation: Jedes **Team**-Mitglied kann ein IHK-Zertifikat als Externer Datenschutzbeauftragter vorweisen.

Wirtschaftlichkeit: Jeder von uns tritt mit dem Grundsatz an, den Datenschutz bei unseren Kunden so umzusetzen, dass einerseits der Gesetzesrahmen eingehalten wird, andererseits aber die Arbeitsabläufe im Unternehmen so wenig wie nur unbedingt nötig beeinträchtigt werden.

Wir arbeiten mit **24-Stunden-Verfügbarkeit** und **Stellvertreterregelung**.

Wir bieten Ihnen kompetente Unterstützung rund um den Datenschutz:

- > **Risikoanalyse** mit ausführlicher Auswertung und Handlungsempfehlungen
- > **Datenschutzkonzepte**, die speziell für Ihr Unternehmen erstellt werden
- > **Datenschutzschulungen** intern für Ihre Mitarbeiter
- > **externe Datenschutzaudits**
- > **Begleitende Beratung zu Datenschutzfragen**
- > **Datenschutzrichtlinien**, die individuell für Ihr Unternehmen erstellt werden
- > **Aus- und Fortbildung für Datenschutzbeauftragte**
- > **Datenschutz-Handbuch**
- > **externer Datenschutzbeauftragter**

Fragen Sie uns! Wir beraten Sie gerne.

Ihr *Team* Datenschutz

Unsere Vorgehensweise im Einzelnen

1. Ist-Analyse bei Datenschutz und IT-Sicherheit

Unsere Ist-Analyse bei Datenschutz und IT-Sicherheit umfasst 52 Fragen, mit denen wir etwa 80 % der Risiken bei Datenschutz und IT-Sicherheit erfassen. Die Analyse dauert zwischen einer und vier Stunden, je nach Unternehmensgröße. Unsere Kunden erhalten eine umfassende individuelle Auswertung mit einer Beschreibung der Situation, den Risiken, den drohenden Konsequenzen und konkreten Handreichungen.

2. Angebot und Berufung als Datenschutzbeauftragter durch den Kunden

Aufgrund der umfassenden Bestandsanalyse erstellen wir ein detailliertes Angebot für Einführung und permanente Umsetzung des Datenschutzes. Mit Erteilung des Auftrags erfolgt die Berufung eines Mitglieds von **Team** Datenschutz zum externen Datenschutzbeauftragten. Sie werden überrascht sein, wie günstig umfassender und verlässlicher Datenschutz sein kann.

3. Auftaktmeeting mit dem Führungsteam, abstimmen der Projektedaten

Dieses Auftaktmeeting dient der Festlegung der Eckdaten für das Projekt Datenschutz und IT-Sicherheit. Es ist straff organisiert und gibt den Verantwortlichen Einblick in die grundsätzliche Vorgehensweise.

4. Analyse und Beschreibung der Geschäftsprozesse, bei denen personenbezogene Daten betroffen sind/ Verfahrensverzeichnis

Grundlage für die Umsetzung von Datenschutz und IT-Sicherheit ist die Kenntnis aller Geschäftsprozesse, bei denen mit personenbezogenen Daten gearbeitet wird. Da diese Geschäftsprozesse in der Regel zum ersten Mal analysiert werden, können wir auf Wunsch auch Hinweise zur Optimierung der Geschäftsprozesse in der Verwaltung geben.

In vielen Fällen wird der Aufwand für den Datenschutz damit zumindest neutralisiert. Die Dauer der Tätigkeit vor Ort im Unternehmen hängt wesentlich davon ab, ob und wie ausführlich die Verfahrensbeschreibungen vorliegen. In jedem Unternehmen gibt es mindestens drei Verfahren: Kundendaten, Mitarbeiterdaten, Lieferantendaten.

5. Analyse des Stands der technisch-organisatorischen Umsetzung bei Datenschutz und IT-Sicherheit

Hier werden die allgemeinen Gefährdungen für Datenschutz und IT-Sicherheit analysiert, z.B. durch ungesicherte USB-Ports, durch unzureichende Sicherheitskonzepte, privates Mailen und privates Surfen am Arbeitsplatz usw. Insbesondere die möglichst ökonomische Umsetzung der im Datenschutzgesetz geforderten technisch-organisatorischen Maßnahmen wird hier angestoßen.

- 6. Risikoanalyse und Erstellen bzw. Ergänzen eines Sicherheitskonzepts**
Dieser Schritt dient der Ermittlung der Sicherheitsrisiken für IT-Anlage und Datenschutz. Wir bieten unseren Kunden an, hierfür einen Führungs-Workshop zum Risikomanagement durchzuführen. Gemeinsam können wir dabei die wesentlichen Risiken und die möglichen Gegenmaßnahmen analysieren. Dieser Schritt ist verbunden mit einer Ortsbegehung.
- 7. Erstellen der Datenschutzrichtlinien**
Nun werden die Datenschutzrichtlinien erstellt und gemeinsam dem Unternehmen übergeben.
- 8. Schulung der Mitarbeiter**
Laut Bundesdatenschutzgesetz sind die Mitarbeiter in geeigneter Weise zu schulen. Der Zeitaufwand ist je nach Vorkenntnissen unterschiedlich.
- 9. Regelmäßige Audits**
In regelmäßigen Abständen, normalerweise zweimal jährlich, prüfen die Datenschutzbeauftragten vor Ort die Umsetzung der Datenschutzrichtlinien.
- 10. Bei Bedarf: Anpassen der Verfahrensbeschreibungen und der Datenschutzrichtlinien, Vorabkontrollen bei geplanten neuen Verfahren**
Wenn die Verfahrensbeschreibungen sich verändert haben und aktualisiert werden müssen, stimmen wir die weitere Vorgehensweise mit der Geschäftsführung ab. Gleiches gilt, wenn neue Verfahren (z.B. Datenbankanwendungen) geplant sind hinsichtlich der durchzuführenden Vorabkontrollen.
- 11. Stillschweigen**
Alle Datenschutzbeauftragten unterliegen einer umfassenden gesetzlichen Schweigepflicht. Eine Verletzung dieser Schweigepflicht hat strafrechtliche Verfolgung zur Konsequenz. Unsere Kunden können sicher sein, dass alle Mitglieder von Team Datenschutz diese Schweigepflicht strikt einhalten.
- 12. Fortbildung**
Unsere Mitglieder besuchen regelmäßig Fortbildungen.
- 13. Haftung**
Alle Mitglieder von Team Datenschutz haben eine Vermögensschadenhaftpflichtversicherung abgeschlossen.
- 14. Prüfung durch Aufsichtsbehörden**
Wir handeln bei der Umsetzung des Datenschutzes nach den Prinzipien der Wirtschaftlichkeit und beachten die Prüfkriterien, die durch die Aufsichtsbehörden für den Datenschutz bei Außenprüfungen angelegt werden. Diese Außenprüfungen erfolgen regelmäßig, wenn ein Betroffener sich wegen vermuteter Datenschutzverletzungen an die Aufsichtsbehörde wendet oder teilweise auch anlassfrei als Routineprüfung.

Risikoanalyse Datenschutz im Unternehmen

Auswertung

Nr. und Themenblock	grün	gelb	rot	Risiko
1. Gebäudesicherheit	0	0	5	100,0 %
2. IT-Sicherheit – Software / Hardware	0	0	5	100,0 %
3. IT-Sicherheit – Verfahren	3	2	3	62,5 %
4. Datenschutzbeauftragter	0	0	7	100,0 %
5. Verfahrensverzeichnis	1	0	2	66,7 %
6. Betroffenen-Information	1	0	2	66,7 %
7. Datenschutz-Richtlinie	3	1	5	66,7 %
8. Schulung / Information der Mitarbeiter	0	0	5	100,0 %
9. Vorabkontrollen	1	0	3	75,0 %
10. Datenschutz-Schnittstellen	0	1	2	100,0 %
Gesamtbewertung	9	4	39	82,7 %

(Beispielunternehmen)

Hier sehen Sie einen kleinen Auszug aus der umfangreichen Risikoanalyse. Diese umfasst 52 Fragen zu den hier genannten Themen, von Gebäudesicherheit bis hin zu den Datenschutz-Schnittstellen. Die Auswertung beinhaltet erste konkrete Schritte, die Sie bei der Umsetzung beachten sollten und umfasst etwa 70 Seiten.

Hier sind nur einige Beispiele genannt.

Frage

Haben Sie Ihren Mitarbeitern schriftlich untersagt, am Arbeitsplatz private E-Mails zu schreiben und zu empfangen?

Ihre Antwort auf diese Frage war „Nein“

Situation: Sie haben den Mitarbeitern (bisher) nicht untersagt, private E-Mails auf ihrem Firmen-PC zu schreiben und zu empfangen – hier die wichtigsten Risiken, die aus dieser Entscheidung erwachsen.

Rechtliche Situation: Vielen Arbeitgebern ist nicht bewusst, welches die Folgen sind, wenn sie ihren Mitarbeitern am Arbeitsplatz privates Surfen im Internet und den privaten E-Mail-Verkehr erlauben. Rein rechtlich haben sie dann den Status eines Internet-Providers. Entsprechendes ist im Telekommunikationsdienstrecht geregelt.

Erhebliche rechtliche Risiken: Mit dem Zugang zum Internet ist das Unternehmen nicht nur zum Provider geworden, oft ohne das zu wissen, aber dennoch im Zweifelsfall mit den vollen Konsequenzen bedroht. Weitere rechtliche Risiken drohen, so z.B. Urheberrechtsverletzungen, wenn Mitarbeiter beim Surfen Software aus dem Internet herunterladen, die dann auf unternehmenseigenen Rechnern gespeichert ist, ohne dass Lizenzen dafür vorliegen.

Wer für seine Mitarbeiter die Hand ins Feuer legt, kann sich sehr leicht verbrennen. Sollten z.B. auf einem unternehmenseigenen Rechner kinderpornographische Inhalte gespeichert sein, haftet die Unternehmensleitung strafrechtlich in voller Höhe. Dies gilt auch, wenn von einem unternehmenseigenen Rechner z.B. Texte mit rechtsradikalen Inhalten in Foren eingestellt werden. In solchen Fällen kann eigentlich nur noch helfen, wenn man nachweisen kann, dass man selbst die Sorgfaltspflicht gewahrt hat, sprich, geeignete Maßnahmen zur Vermeidung solcher Vorfälle ergriffen hat. Kann ein solcher Nachweis nicht geführt werden, stehen die Chancen sehr schlecht, die eigene Unschuld zu beweisen.

Betriebswirtschaftliches Risiko: Einmal abgesehen von der wertvollen Arbeitszeit, die dabei verloren geht, bestehen hier auch hinsichtlich des Datenschutzes Risiken. Erstens können auch mit privaten Mails Viren oder andere Schädlinge ins Unternehmen gelangen und zweitens können auf diesem Weg auch personenbezogene Daten aus dem Unternehmen heraus gelangen.

Datenschutz: Bei der Nutzung von E-Mail und anderen Internetdiensten durch die Beschäftigten sind die eingesetzten Verfahren technisch so zu gestalten, dass von vornherein so wenige personenbezogene Daten wie möglich verarbeitet werden (Grundsatz von Datenvermeidung und Datensparsamkeit).

Bei privaten E-Mails gilt: Der Arbeitgeber ist den Beschäftigten gegenüber zur Einhaltung des Telekommunikationsgeheimnisses verpflichtet. Daher gelten die gleichen Bedingungen wie beim privaten Telefonieren (Fernmeldegeheimnis, Kontrolle nur sehr eingeschränkt möglich).

Dienstliche Mails: Anders bei ausschließlich dienstlich veranlasstem Mailverkehr. Von ein- und ausgehenden dienstlichen E-Mails seiner Beschäftigten darf der Arbeitgeber im selben Maße Kenntnis nehmen wie von deren dienstlichem Schriftverkehr. Beispielsweise könnte der Vorgesetzte verfügen, dass ihm jede ein- oder ausgehende E-Mail seiner Mitarbeiter zur Kenntnis zu geben ist.

Dringende Empfehlung: Einzige sichere Möglichkeit, den Providerstatus mit allen Rechten und vor allem Pflichten zu verhindern, **ist daher den Mitarbeitern schriftlich zu untersagen, am Arbeitsplatz privat zu mailen.**

Tipp: Viele Arbeitnehmer empfinden es heute als normal, während der Dienstzeit auch kleinere private Besorgungen zu erledigen. Das gilt auch und gerade beim Internet.

Hier ist es nützlich, an gut einsehbarer Stelle (vermeidet allzu langen Aufenthalt dort) im Betrieb einen PC aufzustellen, an dem auch privat gesurft und gemailt werden darf. Dadurch kann eine arbeitnehmerfreundliche Regelung getroffen werden, ohne dass die Nutzung ausufert. Da es sich dann auch nicht um den persönlichen Arbeitsplatz des Mitarbeiters handelt, sind die Rechtsfolgen abgemindert, denn an einem für alle zugänglichen Computer ist das Risiko, Provider zu sein, deutlich geringer als wenn an jedem Arbeitsplatz gesurft und gemailt werden kann und darf.

Frage

Ist der Raum, in welchem der zentrale Server untergebracht ist, ausreichend gegen Feuer, Vandalismus usw. geschützt?

Ihre Antwort auf diese Frage war „Ja“

Situation: Sie schützen den Raum, in dem der zentrale Server untergebracht ist, ausreichend gegen Gefahren der Zerstörung.

Bewertung: Sehr vorausschauend – gut, dass Sie diesen sensiblen Bereich im Blickfeld behalten.

Restrisiko: Die Frage bleibt, was „ausreichend“ geschützt ist – natürlich müssen hier Aufwand und Nutzen in einem vernünftigen Verhältnis zueinander stehen.

Handlungsempfehlung: Aber gerade weil der Serverraum so wichtig ist, sollte in regelmäßigen Abständen geprüft werden, ob der Schutz dieses Raumes noch zeitgemäß ist.

Frage

Sind die USB-Steckplätze an den PCs gesichert (nicht genehmigte USB-Sticks oder USB-Geräte werden von den PCs nicht akzeptiert)?

Ihre Antwort auf diese Frage war „Nein“

Situation: Sie haben mit „Nein“ geantwortet – das heißt, dass in Ihrem Unternehmen derzeit keine Maßnahmen zum Schutz der USB-Ports an den Computern ergriffen worden sind.

Bewertung: Sie befinden sich damit in zahlreicher Gesellschaft.

Risiko: In mehr als 90 % der Unternehmen wurden die Gefahren bislang nicht erkannt, die durch nicht gesicherte USB-Ports drohen können. Mit Speichersticks und anderen Hardware-Komponenten, die über USB-Ports in den Computer eingesteckt werden können, setzt sich das Unternehmen in mehrfacher Hinsicht Sicherheitsrisiken aus.

Risiko Virenbefall: Erstens ist die Gefahr recht groß, dass durch nicht geprüfte Geräte, die über die USB-Ports an das System angeschlossen werden, schädliche Software übertragen werden kann. Je nach Virenprogramm bzw. Trojaner dauert es einige Zeit, bis die Schädlinge von den üblichen Schutzprogrammen entdeckt werden. In der Zwischenzeit – wenige Sekunde Verzögerung können schon genügen – können sie ordentlich Schaden anrichten.

Risiko Datenklau: Zum zweiten gibt es heute eigens präparierte USB-Sticks mit sehr großer Speicherkapazität, die über ein eigenes Betriebssystem verfügen und unmittelbar nach dem Einstecken damit beginnen, nach Datensammlungen zu suchen. Damit ist der Wirtschaftsspionage und dem Adressdatenklau Tür und Tor geöffnet, wenn es Angreifern gelingt, einen solcherart präparierten USB-Stick an irgendeinen ihrer PCs anzustecken.

Risiko Notebooks: Denken Sie bitte auch an Notebooks (z.B. im Außendienst), die häufig über sehr umfangreiche Datensammlungen verfügen und deren USB-Ports oft unzureichend geschützt sind, während das DV-System selbst unter Umständen schon recht gut gesichert wird.

Tipp: Um hier wirkungsvoll gegensteuern zu können, sollten Sie sich überlegen, die USB-Ports so zu blocken, das nur eigens zugelassene Geräte eine Verbindung mit dem PC oder dem gesamten System herstellen können. Hierfür gibt es geeignete Software-Lösungen – und die sind sogar recht günstig.

Handlungsempfehlung: Legen Sie zusammen mit den Fachleuten fest, welche Geräte bzw. welches Zubehör über die USB-Ports auf die Rechner zugreifen dürfen. Identifizieren Sie dann mit den Beteiligten alle USB-Ports, die ein potenzielles Sicherheitsrisiko darstellen.

Lassen Sie von Ihren IT-Experten nach geeigneter Software suchen, die dieses Sicherheitsleck schließt. Installieren Sie diese Software und halten Sie sie aktuell. Dokumentieren Sie die Vorgehensweise für den Fall einer eventuellen Regressforderung, die ein Geschäftspartner an Sie richten könnte, falls doch einmal Viren von Ihrem System ausgehen sollten oder Daten unberechtigt in fremde Hände gelangen sollten und dieser Geschäftspartner einen Vermögensschaden dadurch erleiden sollte.

Unterstützung

Haben Sie weitere Fragen zu diesen komplexen Themen oder benötigen Sie Unterstützung? Unsere Experten von **Team** Datenschutz helfen Ihnen gerne weiter.

Wir sind für Sie da

oder ein **Team**-Mitglied in Ihrer Nähe

EUWIS GmbH -
Team Datenschutz
Wichernstraße 2
76185 Karlsruhe

Tel: 0721/9546846
Fax: 0721/9546848

Internet: www.team-datenschutz.de
Mail: info@team-datenschutz.de

SGP GmbH
Jürgen Mollenkopf
Am Buchrain 7
73312 Geislingen

Tel: 07331/307090
Fax: 07331/3070913

Weitere Standorte

EUWIS GmbH
Sperlingweg 3
74906 Bad Rappenau

Tel.: 07264/960981
Fax: 07264/960983

EUWIS GmbH
Am Hagelsrech 14
66806 Ensdorf

Tel.: 06831/7689777
Fax: 06831/7689779