Ausgabe 03 | Juli 2014

TACTICXNEWSLETTER

TACTICX
innovation | solutions | consulting

>> News

Vorstellung Datenschutzmanager

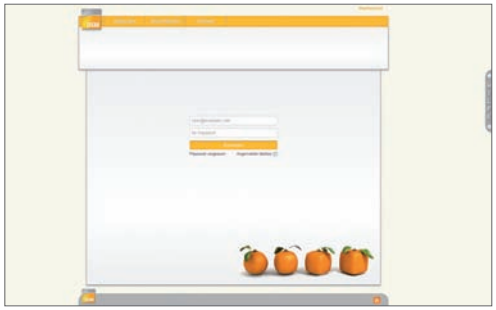
Viele Datenschutzbeauftragte wünschen sich ein effektives Werkzeug zur Unterstützung ihrer täglichen Arbeiten. Ein System, welches nicht nur methodische Unterstützung bietet, sondern auch inhaltliche Hilfestellungen.

Mit dem Datenschutzmanager, kurz DSM, haben wir ein System entwickelt, welches sich an diesen Wünschen orientiert. Im Vordergrund der Entwicklung stand dabei der Grundsatz „easy2use“. Ziel war es ein System zu entwickeln, welches umfangreiche Hilfestellungen bietet und den Datenschutzbeauftragten interaktiv durch gezielte Fragestellungen leitet.

Wir freuen uns, Ihnen nun die erste Beta-Version des Datenschutzmanagers anzukündigen. Im vierten Quartal dieses Jahres wird dann die erste öffentlich zu erwerbende Version folgen. Das System können Sie anschließend gegen eine geringe Monatspauschale nutzen.

Bereits im ersten Release werden wir ein umfangreiches Funktionsangebot bereitstellen. Datenschutzbeauftragte erhalten ein zentrales Tool zur Verwaltung der Audits, Maßnahmen und Aktivitäten. Weiterhin ist ein eLearning Modul integriert, mit dem einfach und effektiv die Mitarbeiter unterwiesen werden können. Zusätzlich leiten interaktive Eingabeassistenten den Benutzer durch komplexe Bereiche und bereiten die Ergebnisse anschaulich auf. Eine Hilfefunktion, welche sowohl für die gesamte Seite als auch für einzelne Eingabefelder zur Verfügung steht, bietet zudem nützliche Hinweise und begleitet Sie über die gesamte Webanwendung.

Die Funktionalität des Datenschutzmanagers wird laufend erweitert und weiterentwickelt. Zudem wird das System inhaltlich durch unsere Datenschutzexperten und Juristen gepflegt, wodurch Sie immer auf dem aktuellen Stand der Rechtsgebung bleiben.



→ **Weitere Informationen zum Datenschutzmanager finden Sie in Kürze auf unserer Homepage *www.tacticx.de*.**
Bei weiteren Fragen können Sie uns natürlich auch gerne persönlich ansprechen.

>> News

Qualitätsstandards bei der tacticx GmbH

Ein wichtiger Unternehmensgrundsatz der tacticx GmbH ist es, einen hohen Qualitätsstandard sicherzustellen. Die Ausbildung unserer Mitarbeiter ist dabei ein wichtiger Aspekt. Unsere Referenten und Berater sind TÜV-geprüfte Datenschutzbeauftragte oder Auditoren und verfügen seit diesem Jahr über eine DIN EN ISO/ IEC 17024 Zertifizierung. Dabei handelt es sich um eine europaweit anerkannte Zertifizierung, die sowohl die Qualität als auch die Kompetenz des Datenschutzbeauftragten auszeichnet. Weiterhin stellt sie momentan die höchste, in Deutschland zu erwerbende, Datenschutz-Auszeichnung dar.

Im Zusammenhang mit der Qualität steht ebenfalls der Faktor Sicherheit. Aus diesem Grund wird auf unserem gesamten Internetauftritt www.tacticx.de das https-Protokoll genutzt. Ihre Daten werden somit auf unserer gesamten Homepage verschlüsselt übertragen.

>> Fachbeitrag *Technische und organisatorische Maßnahmen*

Und keiner will es gewesen sein.

Die technischen und organisatorischen Maßnahmen nach § 9 BDSG bzw. der Anlage zu § 9 BDSG sind hinreichend bekannt. Mit insgesamt acht Maßnahmen hat der Gesetzgeber versucht, eine Art Mindeststandard für den Schutz von personenbezogenen Daten zu schaffen.

Die Liste ist nicht als Empfehlung zu sehen, sondern verpflichtender Bestandteil der gesetzlichen Regelungen. Dabei sind immer alle Maßnahmen umzusetzen.

Folgende Maßnahmen sind im Anhang zu § 9 BDSG zu finden:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle
- Trennungskontrolle

Die meisten dieser Maßnahmen werden im Tagesgeschäft der Unternehmen mehr oder weniger automatisch umgesetzt. So werden wohl alle Unternehmen versuchen, den Zugang zu oder den Zugriff auf schützenswerte Daten einzuschränken oder zu verhindern.

Die Eingabekontrolle fristet allerdings oft eine Art Schattendasein. Bei unseren Audits stellen wir regelmäßig fest, dass die Vorgaben kaum bis gar nicht umgesetzt sind. Aber auch, dass die Notwendigkeit dieser Maßnahme in vielen Unternehmen nicht erkannt wird.

Was genau ist das Ziel der Eingabekontrolle?

Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Anlage (zu § 9 Satz 1) BDSG

Dem Wortlaut der Regelung ist zu entnehmen, dass es sich um eine nachgelagerte Kontrolle handelt. Ziel ist demnach nicht, einen Zugriff zu verhindern, sondern im Nachgang kontrollieren zu können, ob der Zugriff rechtmäßig war. Protokolliert werden müssen alle Eingaben, Veränderungen oder Löschungen von Daten, die einen Personenbezug aufweisen.

Es muss eindeutig nachgewiesen werden können, welche Person die Verarbeitung durchgeführt hat. Eine Eingrenzung auf eine Gruppe ist nicht ausreichend. Aus dieser Vorgabe ergibt sich indirekt, dass Mitarbeiter jeweils einen eigenen, personalisierten Zugang zum IT-System erhalten sollten. Ist dies nicht gegeben, so ist mit weiteren organisatorischen Regelungen zu gewährleisten, dass eine Person eindeutig identifiziert werden kann. Dies kann beispielswiese mit manuellen Protokollen geschehen. Allerdings ist der Aufwand oftmals so hoch, dass besser personalisierte Benutzeraccounts eingerichtet werden sollten.

Auch muss das „Entfernen“ von personenbezogenen Daten dokumentiert werden. Dabei ist das Wort „entfernen“ im BDSG nicht definiert. Es kann aber wohl mit dem Löschen von Daten gleichgesetzt werden. Wichtig in diesem Zusammenhang ist allerdings, dass zwar der Löschvorgang selbst protokolliert werden muss, nicht aber, was gelöscht wurde. Ansonsten würden erneut personenbezogen Daten im Protokoll auftauchen, die aber eigentlich nicht mehr vorhanden sein dürften.

Weiterhin muss eine Auswertung der Protokolle möglich sein. Das heißt, dass irgendjemand die Protokolle, zumindest theoretisch, auswerten kann. Demnach ist festzulegen, wie eine Auswertung erfolgen soll und wer auf die Daten zugreifen darf. Viele Systeme verfügen über automatisierte Auswertungsmöglichkeiten. Ganz aktuelle Anwendungen bieten sogar eine automatische Plausibilitätskontrolle.

Auf den ersten Blick erscheint diese Regelung nachvollziehbar. Auf den zweiten Blick erkennt man allerdings, dass der Gesetzgeber wichtige Details „vergessen“ hat. Der Gesetzgeber spart einen wichtigen Verarbeitungsschritt aus, nämlich das Abrufen und somit den Zugriff auf die Daten. Das Abrufen der Daten ist für die weiteren Schritte, zumindest für das Verändern oder Löschen, notwendig. Je nach Sensibilität der Daten ist eine Protokollierung der Zugriffe dringend anzuraten. So sollte eine Zugriffsprotokollierung z.B. bei allen Krankenhaus- oder Praxisinformationssystemen zum Standard gehören.

Weiterhin schreibt der Gesetzestext nicht vor, dass der Zeitpunkt der Eingabe zu dokumentieren ist. Gefordert ist lediglich nachzuweisen, wer welche Daten verarbeitet hat. Aus den technischen Rahmenbedingungen und dem Schutzzweck der Maßnahme ergibt sich abgeleitet, dass eine Protokollierung ohne Zeitpunkt wenig sinnvoll ist. Eine Nachvollziehbarkeit, geschweige denn eine Prüfbarkeit der Protokolle, ist ohne Zeitstempel nicht gegeben.

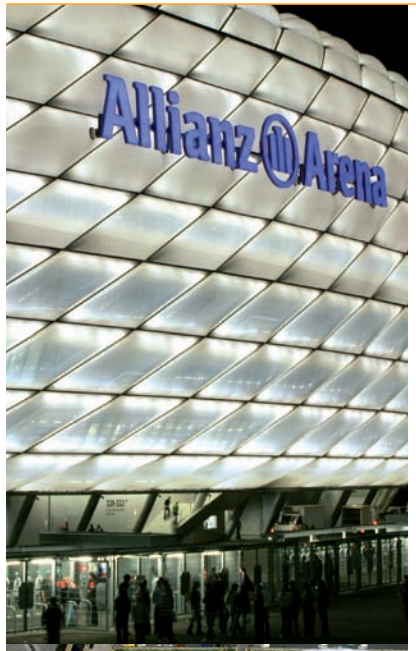
Viele Unternehmen scheuen den technischen Aufwand einer konformen Protokollierung. Je nach Anzahl der Mitarbeiter und Art der Datenverarbeitung können die Protokolldateien schnell einen stattlichen Umfang erreichen. Zusätzlich müssen Regelungen geschaffen werden, wie lange diese Protokolldateien aufbewahrt werden sollen. Auch die Zugriffskontrolle für Protokolle muss geregelt werden. Es soll schließlich nicht jeder Mitarbeiter ohne Einschränkung auf die Protokolle Zugriff haben.

So entstehen technische wie auch organisatorische Aufwände, die einzuplanen sind. Aber warum ist die Eingabekontrolle auch aus Sicht der Unternehmen wichtig und sinnvoll?

Ganz einfach: aus Eigenschutz! Mit einer wirksamen Eingabekontrolle hat ein Unternehmen nicht nur die Möglichkeit Missbrauch aufzudecken, sondern auch Mitarbeiter in die Verantwortung zu nehmen. Anhand von zwei einfachen Beispielen soll abschließend die Notwendigkeit der Eingabekontrolle dargestellt werden.

Stellen Sie sich eine Arztpraxis oder ein Krankenhaus vor. In beiden Einrichtungen werden sehr viele Daten erhoben und erfasst. Nehmen wir nun an, dass sich die Mitarbeiter mit sogenannten Gruppenzugängen an den Systemen anmelden. Es ist also nicht eine einzelne Person identifizierbar, sondern lediglich eine Gruppe, wie z.B. die Sprechstundenhilfen oder Pflegekräfte insgesamt. Werden nun falsche Daten eingegeben, so ist es nicht möglich, eine verantwortliche Person zu identifizieren. Gerade bei der Eingabe von Medikationen ist schnell erkennbar, welche Gefahren entstehen.

Ein weiteres Beispiel haben wir bei unseren Audits leider mehr als einmal angetroffen. Gehen wir mal davon aus, dass die Protokollierung der Verarbeitung in der Buchhaltungssoftware nicht aktiviert wurde. Sei es auf Grund der Datenmenge oder aus Unwissenheit. Wenn nun falsche Daten eingegeben werden, so hat dies sicherlich nicht die gleichen Auswirkungen wie in einer medizinischen Einrichtung. Aber sobald wir z.B. an den Zahlungsverkehr denken, so wird klar, wie hoch die Missbrauchsmöglichkeiten sind. Wenn Zahlungen eingestellt und freigegeben werden, so sollte das Unternehmen aus Eigeninteresse diese Verarbeitung lückenlos nachvollziehen können. Im Fall eines Missbrauchs verliert das Unternehmen ansonsten fast alle Handlungsoptionen. Angefangen vom Schadensersatz bis hin zu arbeitsrechtlichen Konsequenzen. <<



>> News

Datenschutzworkshop in exklusiver Location

In diesem Jahr bieten wir erstmalig das zweitägige Seminar „Praxisworkshop Datenschutz“ an. Wie der Name schon sagt, stehen hierbei Übungen und Beispiele im Vordergrund.

Das Seminar baut dabei auf unser Kompaktseminar betrieblicher Datenschutz auf und vertieft die Inhalte praktisch. Sie erhalten somit wertvolle Tipps, den Datenschutz in Ihrem Unternehmen umzusetzen.

Am ersten Seminartag stehen grundlegende Arbeitsweisen des Datenschutzbeauftragten im Fokus. Anhand eines fiktiven Unternehmens erhalten Sie die Möglichkeit mit praxisbezogenen Übungen Ihr theoretisches Wissen umzusetzen. So wird bspw. ein komplettes Datenschutzaudit durchgeführt.

Der zweite Seminartag ist hingegen einigen speziellen Themen gewidmet, bspw. der Auftragsdatenverarbeitung oder Verfahrensverzeichnissen. Jedes Thema wird dabei an realen Beispielen durchgearbeitet. Weiterhin wird in jedem Seminar ein aktuelles Thema aus den Medien aufbereitet.

Das besondere Highlight an diesem Seminar ist der Veranstaltungsort – die Allianz Arena in München. Genießen Sie während der gesamten Veranstaltung den Blick auf den Stadioninnenraum. Erleben Sie zudem in einer Stadionführung am ersten Seminartag die Mannschaftskabine sowie den Gang durch den Spielertunnel. Die einzigartige Atmosphäre der Allianz Arena macht das Seminar zu einem unvergesslichen Erlebnis.

Mit im Preis von 1299 € zzgl. MwSt. inbegriffen sind zwei Übernachtungen im 4-Sterne Hotel Pullman, die Verpflegung sowie der Transfer zwischen Arena und Hotel. Sie können sich entspannt zurück lehnen, denn wir haben für alles gesorgt.

→ **Die genauen Seminarinhalte sowie weitere Informationen finden Sie unter *https://www.tacticx.de/fortbildung/seminar/praxisworkshop-datenschutz.html*. Melden Sie sich jetzt zu diesem unvergesslichen Erlebnis an.**

Ablauf

1.TAG
- Individuelle Anreise zum Hotel Pullman
- Treffen zum gemeinsamen Kennenlernen

2.TAG
- Abfahrt um 08:15 Uhr
- 09:00 – 15:45 Uhr Seminar inkl. Pausen
- 16:00 Uhr Stadiontour
- 17:30 Uhr Rückfahrt zum Hotel

3.TAG
- Abfahrt um 08:15 Uhr
- 09:00 – 17:00 Uhr Seminar inkl. Pausen
- 17:30 Uhr Rückfahrt zum Hotel
- Individuelle Abreise

* kostenfrei aus dem dt. Festnetz

>> Herausgeber
tacticx GmbH
Zeppelinstr. 26, D-47638 Straelen
Tel. +49 28 34.94 27 70, Fax +49 28 34.94 27 799
https://www.tacticx.de

Bildquellen: (S.2/3) www.fotolia.com, (S.4) Allianz Arena München Stadion GmbH, Arena One GmbH