



Informatik und
Consulting Services

**Mehr Sicherheit.
Mehr Wert.**

Überprüfung der Online ERP-Lösung ERP2 von actindo auf Datenschutzkonformität

Filderstadt, 09.08.10

Unsere Zeichen: So

Seite 1 von 2

Die mittelständische Wirtschaft setzt zunehmend webbasierte Technologien (SaaS, Cloud-Computing) ein. Zum einen können damit Kosten reduziert werden bei andererseits gleichzeitiger Verbesserung der Verfügbarkeit der Systeme. ERP2 von actindo ist eine plattformunabhängige On-Demand-ERP-Lösung, optimiert für Online Shops, die sämtliche Geschäftsprozesse komplett integriert.

Auch ein ERP-System benötigt für die Auftragsabwicklung personenbezogene Daten (Kunden, Lieferanten, etc.). Laut einer Umfrage des Instituts für Demoskopie Allensbach fürchten 54% der deutschen Internet-Nutzer, dass ihre persönlichen Daten im Internet nicht geschützt sind, 31% verzichten sogar auf Einkäufe im Web um ihre Privatsphäre zu wahren. Der Hinweis auf den datenschutzkonformen Betrieb eines Webshops kann daher zu einem deutlichen Vertrauensvorsprung und damit zu einem Wettbewerbsvorteil für den Anbieter führen.

Im Folgenden soll die Datenschutzkonformität beim Einsatz von ERP2 beurteilt werden.

Bewertung der Datenschutzkonformität

Dem Datenschutz unterliegen nur personenbezogene Daten. Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (§ 3 BDSG). Auch eine Auftragsabwicklung benötigt personenbezogene Daten, deren „Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig ist“ – unter Erlaubnisvorbehalt! Die Vorbehalte orientieren sich überwiegend am Gefährdungspotential der Verarbeitung von personenbezogenen Daten.

Auch ERP2 von actindo hat, unzulässig eingesetzt, genauso wie andere Softwarepakete auch, das Potential personenbezogene Daten zu gefährden, z. B.:

- Ein Passwortzugang mit minimal nur sechs Stellen und zeitlich unbegrenzter Gültigkeit,
- Freitextfelder, die es erlauben beliebige personenbezogene Daten zu speichern,
- die Möglichkeit Benutzerprofile ohne Beschränkungen einzurichten,
- ein integriertes Zeiterfassungssystem, das eine Leistungskontrolle möglich macht.

Dem wiederum stehen umfangreiche Maßnahmen gegenüber, die einen datenschutzkonformen Einsatz von ERP2 ermöglichen:

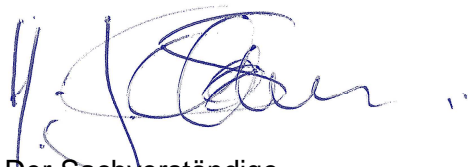
- User-ID und Passwort können durch eine mehrstufige Identifizierung ergänzt werden.
- Dem Anwender wird durch einen Farbbalken die Qualität seines Passworts angezeigt.
- Zeitgesteuerter Logout.
- Benutzerprofile können so eingeschränkt werden, dass jeder einzelne Anwender eigene, sehr spezifische Berechtigungen zugewiesen bekommt.
- Daten werden in einem externen Hochsicherheits-Rechenzentrum in Deutschland auf eigenen Servern gehalten (Serverhousing).
- Ausgeklügeltes vierstufiges Backupkonzept mit regelmäßigem Restoreprozess.
- SSL-zertifizierte Übertragung mit 256-Bit Verschlüsselung.

Um den Anwender zu einem datenschutzkonformen Betrieb von ERP2 anzuhalten wurden weitere Maßnahmen ergriffen:

- Kontextbezogene Warnung vor nicht datenschutzkonformen Auswertungen im Statistikmodul.
- Hinweis auf eine ggf. erforderliche Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten bei der Verarbeitung personenbezogener Daten gem. § 4d Abs. 5 BDSG.
- Hinweis auf die Erfüllung der Vorgaben zur Auftragsdatenverarbeitung gem. § 11 BDSG.
- Kontextbezogene Warnung vor zu schwachen und unsicheren Passwörtern.

Letztendlich ist aber immer der Betreiber einer Website in der Verantwortung, den Einsatz einer Datenverarbeitung datenschutzgerecht zu gestalten. ERP2 bietet ihm dazu die entsprechende Handhabe.

Zum Zeitpunkt der Begutachtung ist daher davon auszugehen, dass ERP2 von actindo datenschutzkonform eingesetzt werden kann.

A handwritten signature in blue ink, appearing to read 'H.-J. Sommer'.

Der Sachverständige
(H.-J. Sommer)