

Aktuelle Entwicklung der Prüfungsanforderungen bzgl. IT-gestützter Rechnungslegungssysteme

Derzeit werden durch den Fachausschuss für Informationstechnologie (FAIT) beim Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW) verschiedene Verlautbarungen vorbereitet, die IT-gestützte Rechnungslegungssysteme betreffen.

[1] Nach Durchsicht der letzten (verfügbaren) Sitzungsprotokolle des FAIT und des Hauptfachausschusses (HFA) soll nachfolgend ein kurzer Überblick über die aktuelle Entwicklung der IDW-Verlautbarungen bzgl. IT-gestützter Rechnungslegungssysteme gegeben werden.

[2] Zur Zeit werden folgende Verlautbarungen erarbeitet bzw. diskutiert:

- IDW-Stellungnahme zur Rechnungslegung "Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren" (IDW RS FAIT x),
- IDW-Prüfungsstandard "Grundsätze ordnungsmäßiger Durchführung von Datenschutzaudits gem. § 9a Bundesdatenschutzgesetz (BDSG)" [IDW PS 870],
- IDW-Prüfungshinweis "Die Prüfung von IT-gestützten Geschäftsprozessen" (IDW PH 9.330.x) in Ergänzung zum IDW-Prüfungsstandard "Abschlussprüfung bei Einsatz von Informationstechnologie" (IDW PS 330),
- Überarbeitung der HFA-Stellungnahme 4/1997 "Projektbegleitende Prüfung EDV-gestützter Systeme",
- Diskussionspapier "IT-Risikomanagement".

IDW-Stellungnahme zur Rechnungslegung "Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren"

[3] Wir haben über den Inhalt, den Stand und den möglichen Erscheinungstermin der IDW-Stellungnahme zur Rechnungslegung "Grundsätze

ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren" derzeit keine weiteren Informationen.

IDW-Prüfungsstandard "Grundsätze ordnungsmäßiger Durchführung von Datenschutzaudits"

[4] Gegenstand des Datenschutzaudits gem. § 9a BDSG ist die Beurteilung der Datenschutzerklärung der datenverarbeitenden Stelle (als Selbsterklärung) durch einen unabhängigen (externen) Sachverständigen.

[5] Die Datenschutzerklärung stellt das Ergebnis der in periodischen Abständen durch das Unternehmen (selbst) durchgeführten "Datenschutzbetriebsprüfungen" dar. Diese vom Unternehmen verfasste selbst Datenschutzerklärung ist Gegenstand der Prüfung und Zertifizierung durch einen unabhängigen (externen) Datenschutzgutachter gem. § 9a BDSG. Bei dieser Zertifizierung gem. § 9a BDSG handelt es sich nicht um eine Systemprüfung i.S.d. IDW-Prüfungsstandards "Prüfungsnachweise im Rahmen der Abschlussprüfung" (IDW PS 300) bzw. IDW PS 330, sondern um die **Durchführung einer prüferischen Durchsicht** analog IDW-Prüfungsstandard "Grundsätze für die prüferische Durchsicht von Abschlüssen" (IDW PS 900).

[6] Bei der prüferischen Durchsicht erfolgt eine kritische Würdigung der Sachverhalte auf Grundlage von Plausibilitätsbeurteilungen. Die Durchsicht ist so zu planen und durchzuführen, dass mit einer **gewissen Sicherheit** eine **negativ formulierte Aussage** getroffen werden kann.

[7] Die "Datenschutzbetriebsprüfung" als interne periodische Datenschutzprüfung wird von § 9a BDSG nicht näher erläutert. Die Vorgehensweise bei dieser Prüfung ähnelt der einer gem. IDW-Prüfungsstandard "Das interne Kontrollsystem im Rahmen der Abschlussprüfung" (IDW PS 260) bzw. IDW PS 330 durchzuführenden **Systemprüfung**.

[8] Gegenstand dieser "Datenschutzbetriebsprüfung" ist

- das Datenschutzkonzept,
- die Datenschutzpolitik sowie
- das Datenschutzprogramm und
- das Datenschutzmanagementsystem.

[9] Das **Datenschutzkonzept** legt aus Sicht der gesetzlichen Vertreter den zu erreichenden Grad an Datenschuttsicherheit (Schutzbedarf) fest. Darüber

hinaus werden die daraus abzuleitenden Anforderungen an die Datenschutzpolitik und an den Prozess zur kontinuierlichen Verbesserung des Datenschutzes festgelegt.

[10] Auf Grundlage der Bestandsaufnahme der datenschutzrelevanten Prozesse und geltenden datenschutzrechtlichen Vorschriften ist eine schriftlich zu fixierende **Datenschutzpolitik** (Strategie) zu entwickeln. Basierend auf der Datenschutzpolitik ist das Datenschutzprogramm umzusetzen und das Datenschutzmanagementsystem einzurichten.

[11] Das **Datenschutzprogramm** konkretisiert die Datenschutzziele und umfasst den Katalog konkreter Maßnahmen und den Fristenplan zur Umsetzung der Datenschutzpolitik.

[12] Das **Datenschutzmanagementsystem** (internes Kontrollsystem; IKS) legt die Regeln, Richtlinien, Maßnahmen, Ressourcen (Hard- und Software, Personal etc.), Verfahren, Zuständigkeiten, Abläufe und Organisationsstrukturen zur Umsetzung und Überwachung des Datenschutzprogramms fest.

[13] Zur Zeit nicht abschließend geregelt sind wesentliche Aspekte der Datenschutzprüfung gem. § 9a BDSG, nämlich:

- Das **Sollobjekt der "Datenschutzbetriebsprüfung"**. Die vom Gesetzgeber avisierte Prüfungsverordnung ist bisher (auf Bundesebene) noch nicht erlassen worden.
- Die **Registrierung von Datenschutzprüfern**. Derzeit ist keine staatliche Stelle vorhanden, die eine Akkreditierung als Datenschutzprüfer möglich macht.
- Der **Prozess der Datenschutz-Siegelvergabe**. Die notwendigen Voraussetzungen für eine Siegelvergabe sind ebenfalls (zur Zeit) nicht vorhanden.

[14] Die offenen Punkte sind derzeit Gegenstand von Gesprächen zwischen dem IDW / FAIT und dem Bundesdatenschutzbeauftragten, in denen auch der Stand der Überlegungen seitens des IDW / FAIT der Bundesregierung erörtert werden soll. Über die Ergebnisse der durchgeführten Gespräche liegen uns derzeit keine weiteren Informationen vor.

IDW-Prüfungshinweis "Die Prüfung von IT-gestützten Geschäftsprozessen"

[15] Zur Veranschaulichung der Prüfung von IT-gestützten Geschäftsprozessen wird derzeit ein IDW-

Prüfungshinweis in Ergänzung zum IDW PS 330 erarbeitet.

[16] Ziel des neuen Prüfungshinweises ist es, anhand beispielhafter Kerngeschäftsprozesse, die Prüfungsmethodik des IDW PS 330 und die daraus abzuleitende Vorgehensweise bei der Prüfung IT-gestützter Geschäftsprozesse zu verdeutlichen.

HFA-Stellungnahme 4/1997 "Projektbegleitende Prüfung EDV-gestützter Systeme"

[17] Grundlegendes Ziel projektbegleitender Prüfungen ist, sicherzustellen, dass neu entwickelte, geänderte oder erweiterte IT-gestützte Rechnungslegungssysteme den Grundsätzen ordnungsgemäßer Buchführung (GoB) entsprechen und somit die Voraussetzungen für die Ordnungsmäßigkeit der Buchführung als Grundlage für die Abschlusserstellung gegeben ist.

[18] Die derzeit vorliegende HFA-Stellungnahme 4/1997 "Projektbegleitende Prüfung EDV-gestützter Systeme" basiert noch auf der FAMA-Stellungnahme 1/1987 i.d.F 1993, die bereits seit 2002 durch IDW-Rechnungslegungsstandard "Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie" (IDW RS FAIT 1) und den IDW PS 330 ersetzt wurde.

[19] Eine Überarbeitung ist notwendig, da komplexe IT-gestützte Rechnungslegungssysteme nahezu vollständig in die betrieblichen Informationssysteme integriert sind und es daher sachgerecht erscheint, die im IDW PS 330 dargestellte **prozessorientierte Prüfungsmethodik** entsprechend anzuwenden. Zudem wird die Stellungnahme modernisiert und an die Änderungen im IDW RS FAIT 1 angepasst (insb. Begriffsdefinitionen).

Diskussionspapier "IT-Risikomanagement"

[20] Das Diskussionspapier ist derzeit noch in Bearbeitung.

[21] Nach unserem Kenntnisstand wird seitens des IDW derzeit überlegt, ob das Diskussionspapier als Beitrag im WP-Handbuch aufgenommen werden soll. Damit eröffnete sich die Möglichkeit, das Thema breiter darzustellen und anhand von Beispielen zu verdeutlichen.

Quelle: verschiedene Protokolle des FAIT und des HFA

Stand: 20.01.2005