SIEMER PARTNER

Sind Ihre Geschäftsprozesse und Ihre IT-Security datenschutzkonform?

Wie Sie Ihr Wirtschaftsprüfer bei der Einhaltung der Regeln unterstützt

AGENDA

I. Risikoorientierter Prüfungsansatz

II. Abschlussprüfung und EU-DSGVO

I. Risikoorientierter Prüfungsansatz

- Ausgangspunkt: Gewinnung eines Verständnisses von dem Unternehmen sowie dessen rechtlichem und wirtschaftlichem Umfeld

➢ Kennenlernen der Aufbau- und Ablauforganisation

➢ Aufnahme der kritischen Geschäftsprozesse, sog. „IKS-Prüfung“ („IST“)

➢ Analyse dieser Geschäftsprozesse auf ihre angemessene Ausgestaltung („SOLL“)

➢ Prüfung dieser Geschäftsprozesse auf ihre Funktionsfähigkeit

I. Risikoorientierter Prüfungsansatz

Beispiel:

Personalbuchhaltung

I. Risikoorientierter Prüfungsansatz

- Zunahme IT-gestützter Geschäftsprozesse

➢ Prüfung rechnungslegungsrelevanter IT-Systeme unerlässlich

II. Abschlussprüfung und EU-DSGVO

- Zwischenfazit: Durch den risikoorientierten Prüfungsansatz analysiert der Prüfer Geschäftsprozesse, interne Kontrollen und Systeme mit dem Primärziel, Schwächen, die sich auf die „Richtigkeit“ des Jahresabschlusses auswirken könnten, zu identifizieren
- Aber: Es entstehen darüber hinaus auch Kenntnisse über das Unternehmen, die über das Urteil über den Jahresabschluss hinausgehen, denn
  - Der Abschlussprüfer verschafft sich im Rahmen seiner Prüfung ein Bild ihrer Datenverarbeitungssysteme
  - Es bestehen Überschneidungen mit grundsätzlichen Regelungen der EU-DSGVO, denn auch der Abschlussprüfer prüft im Kern die Datensicherheit

II. Abschlussprüfung und EU-DSGVO

- Betrachten wir das Beispiel aus dem Bereich Lohn und Gehalt:
  - Die Datenschutzgrundverordnung verlangt, dass kein Unbefugter Zugriff auf „fremde“ Daten (Personaldaten) bekommt.
  - Der Abschlussprüfer muss prüfen, ob z.B. ein Unbefugter Zugriff auf die Personalbuchhaltung hat, um Fehlerquellen und oder Betrugsmöglichkeiten zu identifizieren
  - In Beiden Fällen steht der Systemzugang im Mittelpunkt: **W**er darf **W**ann **W**as **W**arum?
  - Übliche Fragestellungen bei der Prüfung des Systemzugangs:
    - Wo steht der Server und wer hat physischen Zugriff auf die Hardware?
    - Welche Rollen gibt es im System? (z.B.: Super-User, Buchhaltung, Lohnbuchhaltung, Geschäftsleitung, Administrator, …)
    - Welche Rechte sind den Rollen zugeordnet?
    - Welcher Mitarbeiter hat welche Rollen?
    - Wer kennt das Administrator / Super-User Passwort?
  - Kleiner Check: Wie oft und durch wen erfolgte eine Anmeldung als „Super-User“?
- Was passiert nun, wenn die Prüfung des Systemzugangs Schwächen oder sogar Gesetzesverstöße offenbart?

II. Abschlussprüfung und EU-DSGVO

- Schwächen innerhalb der rechnungslegungsrelevanten Geschäftsprozesse werden an die Geschäftsleitung kommuniziert
- Gesetzesverstöße (z.B. gegen die EU-DSGVO), auch wenn Sie nicht rechnungslegungsrelevant sind, werden an die Geschäftsleitung kommuniziert

II. Abschlussprüfung und EU-DSGVO

- Mehrwert der Abschlussprüfung für den Unternehmer
  - Analyse und Aufnahme der rechnungslegungsrelevanten Geschäftsprozesse durch den Abschlussprüfer im Rahmen der Jahresabschlussprüfung
  - Erweiterung des Prüfungsauftrages möglich:
    - „Schauen Sie sich bitte auch … an!“
  - Kommunikation aufgedeckter Schwächen auch außerhalb der rechnungslegungsrelevanten Geschäftsprozesse, z.B. im sogenannten „Management Letter“
  - Unterbreiten von Verbesserungsvorschlägen auf Basis unserer Kenntnisse und Erfahrungen
    - „Wie machen das eigentlich die Anderen?“
  - Einbindung des Abschlussprüfers bei der Neueinrichtung oder Überarbeitung der IT-gestützten Geschäftsprozesse

Vielen Dank für Ihre Aufmerksamkeit

Markus Buhlrich

Dipl.-Oec., Wirtschaftsprüfer,
Steuerberater

Jasmin Bottermann

Dipl.-Kffr., Wirtschaftspüferin,
Steuerberaterin

SIEMER + PARTNER
Partnerschaft mbB
Otto-Lilienthal-Straße 14
D-28199 Bremen

Tel.: +49 421 33763-0
Fax: +49 421 33763-47
E-Mail: info@siemerundpartner.de
www.siemerundpartner.de