Packen wir’s an:
Neufassung der GoBD verstehen und technisch umsetzen

18. September 2025

Berno Zimmerer (Zimmerer StBG mbH & Co. KG)
Stefan Kaumeier (dekodi GmbH)

TaxTec@work

Agenda

- GoBD 2019 im Fokus der digitalen Belege
- GoBD 2024 im Fokus der digitalen Belege
- Anpassung GoBD 2024: Fokus der Einführung E-Rechnung ab 2025
- Praxis: Datenschutz E-Rechnung
- Praxis: Probleme seit Einführung E-Rechnung 2025
- Praxis: IDW - Cloud

GOBD 2019:
IM FOKUS DER DIGITALEN BELEGE

TaxTec@work

GoBD 2019: im Fokus der digitalen Belege

Hauptschreiben vom 28.11.2019

- Komplette Neufassung und Ersatz BMF vom 14.11.2014
- „Cloud“ einbezogen (Rz. 20)
- Faktura-Systeme einbezogen (Rz. 20)
- Aufbewahrung sog. „Mehrstücke“ bei Hybride RG-Formate z.B. ZUGFeRD, Factur-X
- Sicherstellung von „technischen und organisatorischen Kontrollen“ für Erfassung von Geschäftsvorfällen
- Elektronische Belege = Aufbewahrung im elektronischen Format
- Keine Aufbewahrung von E-Mails mit ges. Anlage E-Rechnung

GOBD 2024:
IM FOKUS DER DIGITALEN BELEGE

TaxTec@work

GoBD 2024: Im Fokus der digitalen Belege

Änderungen vom 11.03.2024

- Div. kleiner klarstellende Anpassungen
- Neufassung Datenüberlassung Z3
- Digitale LohnSchnittstelle
- Exporte aus eAS

ANPASSUNG GOBD 2024:
FOKUS DER EINFÜHRUNG E-RECHNUNG AB 2025

TaxTec@work

Anpassung GoBD 2024: Fokus der Einführung E-Rechnung ab 2025

Änderungen vom 14.07.2025

- Grund: Einführung E-Rechnung B2B im Inland ab 2025
- Div. technische klarstellende Anpassungen
- Faktura: (Rz. 76) – keine doppelte Archivierung bei Rechnungsausgang mehr erforderlich
  Keine bildhafte Kopie der Ausgangsrechnung (PDF-Datei) mehr zu speichern bzw. aufzubewahren,
  wenn jederzeit auf Anforderung eine inhaltlich identisches Mehrstück der Ausgangsrechnung erstellt werden kann.
  ➔ Fokus auf Sicherung/Archivierung der Faktura-Dateien
- Buchungsbeleg als strukturierter Datensatz (z.B. E-Rechnung) (Rz. 118),
  dann keine bildliche, sondern nur noch eine inhaltliche Übereinstimmung erforderlich
  (entgegen § 147 Abs. 2 Nr. 1 AO)
  ➔ Unterstützung echte Automatisierung, Vermeidung von Speicherplatz

Anpassung GoBD 2024: Fokus der Einführung E-Rechnung ab 2025

- Hybride RG-Formate (RZ 119)

  Aufbewahrung ausreichend, wenn nur strukturierte Teil archiviert wird; z.B. PDF-Teil.
  Jedoch nur, wenn PDF keine zusätzlichen oder abweichenden Informationen enthält, welche für Besteuerung erforderlich sind. Beispiel: Buchungsvermerke

  ➔ Fokus auf automatisierte Buchhaltung mittels Datensätze, ohne zusätzlich bildhafte Ergänzungen; bildhafte Ergänzungen führen zur Hemmung echter Digitalisierung

- Technische Zahlungsbelege (RZ 121)

  Reine Transaktionsnachweise, etwa Belege von Kartenterminals oder Zahlungsdienstleistern, müssen nicht archiviert werden, wenn sie nicht als Buchungsbeleg dienen. Nur wenn sie die einzige Abrechnungsgrundlage sind oder für die steuerliche Einordnung (z. B. bar/unbar) erforderlich sind.

  ➔ Fokus liegt i.d.R. auf dem Datensatz; erstmalige Rechtssicherheit

Anpassung GoBD 2024: Fokus der Einführung E-Rechnung ab 2025

- Aufbewahrung Datenformate (RZ 131)
  - Belege müssen in dem Format, in welchem sie eingegangen sind, archiviert werden
  - Eine Konvertierung (Umwandung) in ein anderes Format ist zulässig.
    Vorgaben Rz. 135 zu beachten.
    Bei OCR z.B. Datev DUO: Anreicherung von Bildinformationen müssen archiviert werden
  - Aufbewahrung strukturierten Teil der E-Rechnung ausreichend.
    Strukturierter Teil muss Vorgaben von § 14 Absatz 1 Satz 3 und 6 UstG enthalten.
    Weitere Archivierung erforderlich, wenn für Besteuerung von Bedeutung (z.B. qualifizierte Signaturen, Buchungsvermerke, etc.).

➔ **zukünftig auf echte Automatisierung setzen; strukturierte Belege; selbst gestrickte Prozesse beim Unternehmen vermeiden bzw. anpassen**

Anpassung GoBD 2024: Fokus der Einführung E-Rechnung ab 2025

- Neufassung „Mittelbarer Datenzugriff (Z2)“ (RZ 166)
  - Unternehmer müssen, nach Vorgaben der Finanzverwaltung selbst, die Auswertungen für den Prüfer liefern
  - In einem maschinell auswertbaren Format (neu)
  - Alternativ ist eine sog. „Nur-Lesezugriff“ auch möglich (bisher)

➔ es darf keine neue Software programmiert werden dürfen; alternativ direkter Datenzugriff

Exkurs:

Z1: Unmittelbarer Zugriff

Z2: Mittelbarer Zugriff

Z3: Datenträgerüberlassung

TaxTec@work

PRAXIS: DATENSCHUTZ E-RECHNUNG

TaxTec@work

Praxis: Datenschutz E-Rechnung

Cyberbetrug durch manipulierte Rechnungen

- Aufgabe des Unternehmers Datenklau bzw. Gefahr RG-Manipulation zu vermeiden
- OLG Schleswig-Holstein vom 18.12.2024 - AZ. 12 U 9/24:
  - Keine schuldbefreite Zahlung auf manipuliertes Konto
  - Unternehmer müssen Rechnungsversand im Sinne der DGSVO absichern
  - Gute Praxishinweis auf nächster Folie – Auszug aus https://b2.legal/
- Evtl. Abhilfe ab 09.10.2025 bei Sepa-Überweisungen in der EU

  Ab dem 9. Oktober 2025 müssen Banken bei SEPA-Überweisungen in der EU den Empfängernamen mit der angegebenen IBAN abgleichen, ein Verfahren namens Verification of Payee (VoP).

Praxis: Datenschutz E-Rechnung

Unternehmer tragen Mitverantwortung für die Sicherheit des Rechnungsversands

- Das Gericht betonte, dass Unternehmen verpflichtet sind, ihre E-Mail-Kommunikation abzusichern.
- Unverschlüsselte oder nur transportverschlüsselte E-Mails (z. B. über TLS) gelten als unsicher.
- Es wird erwartet, dass Unternehmen Maßnahmen wie Ende-zu-Ende-Verschlüsselung, digitale Signaturen oder die Bereitstellung von Rechnungen über sichere Kundenportale nutzen.

Haftung bei Verstößen gegen die DSGVO

- Falls ein Unternehmen nicht für ausreichende Sicherheitsmaßnahmen sorgt, kann es gegen die Datenschutz-Grundverordnung (DSGVO) verstoßen.
- In diesem Fall kann dem Kunden ein Schadensersatzanspruch zustehen, der mit der Werklohnforderung des Unternehmens verrechnet werden kann.
- Das bedeutet: Wenn ein Unternehmen keine geeigneten Schutzmaßnahmen ergreift, könnte es im Streitfall die Zahlung verlieren.

Praktische Empfehlungen für Unternehmer

- ✓ Rechnungen nicht unverschlüsselt per E-Mail versenden.
- ✓ Digitale Signaturen oder Kundenportale für Rechnungsstellung nutzen.
- ✓ Ihre Kunden vor Betrugsmethoden (z. B. geänderte Kontodaten) warnen.
- ✓ Auf Rechnungen explizit vermerken, dass Bankverbindungen nicht per E-Mail geändert werden.
- ✓ Kunden sensibilisieren, Zahlungsdaten telefonisch zu bestätigen, wenn sie ungewöhnlich erscheinen.

Auszug aus https://b2.legal/

PRAXIS: PROBLEME SEIT EINFÜHRUNG E-RECHNUNG 2025

TaxTec@work

Praxis: Probleme seit Einführung E-Rechnung 2025

Fehlerhafte E-Rechnungen

- E-Rechnung entspricht nicht den gesetzlichen Anforderungen;
  DIN16931 – semantisches Datenmodell in Programmierung Faktura-Software nicht oder unzureichend umgesetzt;
- Muss-Datenfelder sind nicht gefüllt
- Daten-Inhalte in falschen Datenfelder (z.B. Steuernummer, Zahlungsbedingungen)
- PDF bei Hybriden Formaten stimmt nicht mit XML-Dateninhalt überein; Gefahr Verlust Vorsteuerabzug
- Falsche RG-Inhalte => Validierung von Stammdaten erforderlich

Praxis: Probleme seit Einführung E-Rechnung 2025

Hybride E-Rechnungen mit zu hohen Dateigröße

- 10-jährige Archivierungspflicht führt zu sehr hohen Folgekosten bei Speicherung
- Hinweis auf neues BMF-Schreiben RZ 119 => Vermeidung von Buchungsvermerken auf PDF-Anhängen, somit keine Archivierung erforderlich

Prozesse sind ab 2025 nicht überprüft bzw. angepasst worden

- Einführung von digitalen Belegen führt zu einer Überprüfung der bisherigen Papierprozesse
- Zum Teil werden Papier-Prozesse für digitale Belege verwendet;
  z.B. händische Belegprüfstempel werden fortgeführt
- Veränderung E-Rechnung ab 2025 sollte zum Anlass genommen werden die unternehmens-internen Prozesse der Belegverwaltung sowie der Buchungsprozesse neu zu organisieren;

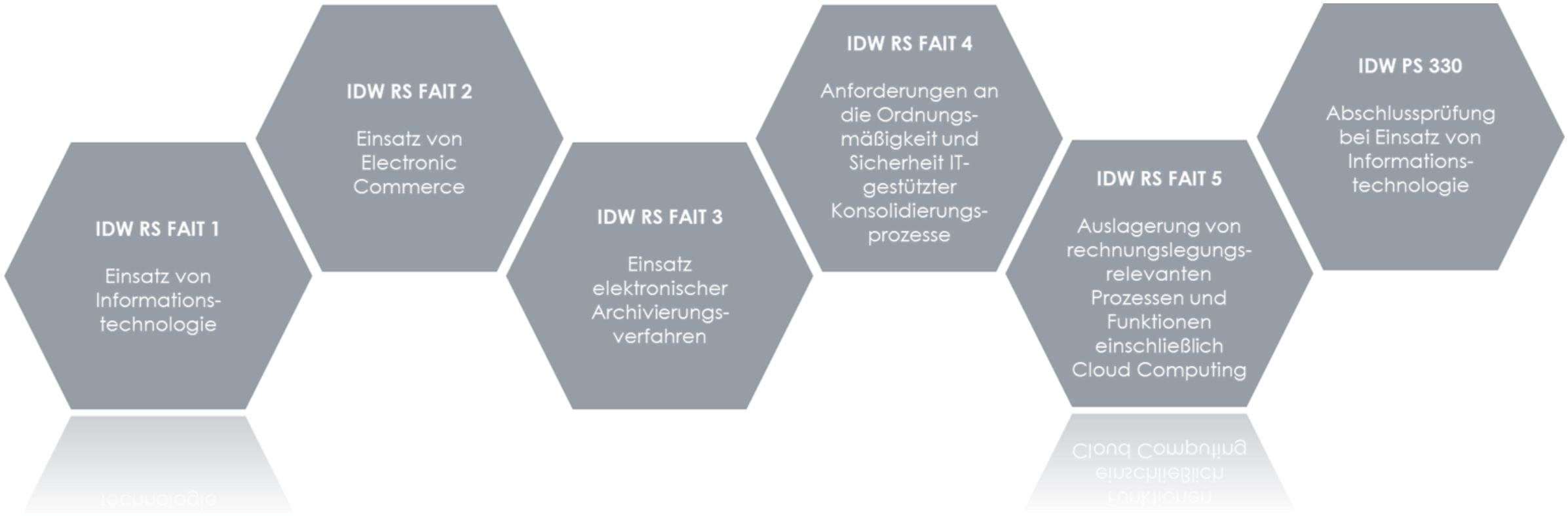
  Stichwort: „Shit in – Shit out“

PRAXIS: IDW - CLOUD

TaxTec@work

Praxis: IDW - Cloud

IDW – div. Verlautbarungen im Fokus der Digitalisierung



TaxTec@work

Praxis: IDW - Cloud

Cloud als Anwendungsmedium

Risikoreport zur Datenspeicherung in der Cloud

- In vielen Betrieben überwiegt Sorglosigkeit.
- **4/5** der Unternehmen speichern sensible Daten in Public-Cloud-Diensten.
- **1/5** mangelt es auch an einem Überblick der Daten, welche in der Cloud abgelegt sind.
- Cyber-Experten weisen darauf hin, dass lediglich **9%** aller Cloud-Services in der Lage sind, gespeicherte Daten zu verschlüsseln.
- Somit sind **91%** aller in Cloud-Services gespeicherten Daten bei einem Sicherheitsvergehen nicht geschützt!
- Private Smartphones und Laptops wurden als Sicherheitsrisiko identifiziert.
- **79%** der Unternehmen erlauben ihnen einen Zugang zur Cloud.

[1]lt. Risikoreport von McAfee vom 28.01.2020

FRAGERUNDE

TaxTec@work