StBK Berlin

Musterklausur mit Lösungshinweisen für die Fortbildungsprüfung Fachassistent/in Digitalisierung und IT-Prozesse

Korrekturbogen/Lösungshinweise

Teil 1:
Abgaben- und verfahrensrechtliche Beurteilung digitaler Arbeitsabläufe, Verfahrensdokumentation, Datenschutz, Automatisierung **(70 Pkt.)**

Teil 2:
Digitale Arbeitsabläufe in der Kanzlei, Digitale Arbeitsabläufe im Mandatsverhältnis, Zusammenarbeit mit Finanzbehörden und Dritten **(30 Pkt.)**

Bearbeitungszeit 180 Minuten

Punkte- und Notenschema

(1) Für den schriftlichen und mündlichen Teil der Prüfung gelten folgende Punkte und Noten:

Punkte	Noten		
100-92	sehr gut	(1)	eine den Anforderungen in besonderem Maße entsprechende Leistung
91-81	gut	(2)	eine den Anforderungen voll entsprechende Leistung
80-67	befriedigend	(3)	eine den Anforderungen im Allgemeinen entsprechende Leistung
66-50	ausreichend	(4)	eine Leistung, die zwar Mängel aufweist, aber im Ganzen den Anforderungen noch entspricht
49-30	mangelhaft	(5)	eine Leistung, die den Anforderungen nicht entspricht, jedoch erkennen lässt, dass die notwendigen Grundkenntnisse vorhanden sind
29-0	ungenügend	(6)	eine Leistung, die den Anforderungen nicht entspricht und bei der selbst die Grundkenntnisse lückenhaft sind

(2) Die Prüfungsleistungen sind mit ganzen Punkten zu bewerten.
(3)

Lösungshinweise für die Korrektoren

Die Lösungshinweise zu dieser Musterklausur für die Fortbildungsprüfung Fach--assistent/in Digitalisierung und IT-Prozesse sind sehr ausführlich gehalten worden und dienen nicht als Standard für kommende Klausurlösungen. Diese werden mithin einen kürzeren Umfang haben.

Aufgaben Teil 1:

1. Lösung (7 Punkte)

Im BMF-Schreiben vom 28.11.2019 nimmt die Finanzverwaltung zur Belegfunktion Stellung. Sie stellt zunächst fest, dass der Grundsatz „Keine Buchung ohne Beleg" unverändert gültig ist. Ist kein Fremdbeleg vorhanden, so ist zwingend ein Eigenbeleg zu erstellen, auch wenn die Buchung scheinbar selbsterklärend ist.

Die Finanzbuchhaltung verlangt für die Erfüllung der Belegfunktion eine weitere Bearbeitung des Dokuments. Gefordert werden bei Papierbelegen Angaben zur Kontierung, zum Ordnungskriterium der Ablage und zum Buchungsdatum auf dem Beleg. Bei elektronischen Belegen können diese Angaben durch Verknüpfung mit entsprechenden Datensätzen erfolgen.
Nach dem o.a. BMF-Schreiben sind folgende Anforderungen an einen digitalen Beleg (Eingangsrechnung) zu erfüllen!

- Eindeutige Belegnummer (z.B. Index, Paginiernummer)
- Belegdatum
- Belegaussteller und -empfänger
- Betrag bzw. Mengen – oder Wertangaben, aus denen sich der zu buchende Betrag ergibt
- Hinreichende Erläuterung des Geschäftsvorfalls
- Währungsangabe und Wechselkurs bei Fremdwährung
- Verantwortlicher Aussteller, soweit vorhanden

2. Lösung (7 Punkte)

Die Ordnungsmäßigkeit elektronischer Bücher und sonst erforderlicher elektronischer Aufzeichnungen ist nach gleichen Prinzipien zu beurteilen wie die Ordnungsmäßigkeit bei manuell erstellten Büchern und Aufzeichnungen.

Das Erfordernis der Ordnungsmäßigkeit erstreckt sich – auch auf damit in Zusammenhang stehenden Verfahren und Bereiche des DV-Systems, da die Grundlage für die Ordnungsmäßigkeit elektronischer Bücher und sonst

erforderlicher Aufzeichnungen bereits bei der Entwicklung und Freigabe von Haupt,- Vor- und Nebensystemen einschließlich des dabei angewandten DV-gestützten Verfahrens gelegt wird.

Nach dem Grundsatz der Unveränderbarkeit (§ 146 Abs. 4 AO) darf eine Buchung oder eine Aufzeichnung nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später geändert worden sind.

Veränderungen und Löschungen von und an elektronischen Buchungen oder Auszeichnungen müssen daher so protokoliert werden, dass die Voraussetzungen des § 146 Abs. 4 AO bzw. § 239 Abs. 3 HGB erfüllt sind. Für elektronische Dokumente und andere elektronische Unterlagen, die gem. § 147 AO aufbewahrungspflichtig und nicht Buchungen oder Aufzeichnungen sind, gilt dies sinngemäß.

3. Lösung (7 Punkte)

Die Aufbewahrungsfrist für digitale Unterlagen beträgt:

für Handelsbücher, Inventare	10 Jahre (§ 257 HGB i.V. mit § 147 Abs. 3 und Abs. 1, Nr. 1 AO
für Buchungsbelege	10 Jahre (§ 257 HGB i.V. mit § 147 Abs. 3 und Abs. 1, Nr. 4 AO)
für empfangene und abgesandte Handels- und Geschäftsbriefe	6 Jahre (§ 257 HGB i.V. mit § 147 Abs. 3 und Abs. 1, Nr. 2, 3 AO)
für Unterlagen bei Uberschusseinkünften über 500.000 €	6 Jahre (§ 147a AO)

Die 10-jährige Aufbewahrungsfrist gilt nicht, wenn die Steuerbescheide noch nicht bestandskräftig sind. Sie verlängert sich entsprechend, soweit die Festsetzungsfrist noch nicht abgelaufen ist (§ 147 Abs. 3, Satz 5 AO).

4. Lösung (7 Punkte)

Die Finanzbehörde hat das Recht, die mit Hilfe eines DV-Systems erstellten und nach § 147 Abs. 1 AO aufbewahrungspflichtigen Unterlagen durch Datenzugriff zu prüfen. Das Recht auf Datenzugriff steht der Finanzbehörde nur im Rahmen der gesetzlichen Regelungen (steuerliche Außenprüfungen und Nachschauen) zu. Durch die Regelungen zum Datenzugriff wird der sachliche Umfang der Außenprüfung (§ 194 AO) nicht erweitert; er wird durch die Prüfungsordnung (§ 196 AO, § 5 BpO) bestimmt.

Werden Bücher und Aufzeichnungen digital geführt, hat die Finanzverwaltung damit im Rahmen einer Außenprüfung oder einer Nachschau das Recht, in die digitalen Daten Einsicht zu nennen. Dieses Recht umfasst nach Auffassung der Finanzverwaltung alle gespeicherten aufbewahrungspflichtigen Unterlagen und Daten und nicht nur die Buchführung bzw. Aufzeichnungen im engeren Sinne.

Für diesen Datenzugriff stehen der Verwaltung drei verschiedene Varianten zur Verfügung. Die Finanzverwaltung kann den Datenschutz auch durch Kombination der zulässigen Methoden ausüben. Die Entscheidung, welche Form des Datenzugriffs genutzt wird, und ob die verschiedenen Möglichkeiten kumulativ verwendet werden, liegt im pflichtgemäßen Ermessen der Behörde. Der Steuerpflichtige ist verpflichtet, die entstehenden Kosten zu tragen und die Finanzverwaltung bei der Prüfung zu unterstützen.

Auch wenn die Finanzverwaltung das Recht auf einen Datenzugriff hat, so besteht für sie keine Verpflichtung digital zu prüfen. Sie kann im Rahmen ihres Ermessens vom Aufbewahrungspflichtigen verlangen, dass er die Unterlagen unverzüglich ganz oder teilweise ausdruckt oder ohne Hilfsmittel lesbare Reproduktionen vorlegt.

4.1. Unmittelbarer Datenzugriff (Z1)

Die Finanzbehörde hat das Recht, selbst unmittelbar auf die Daten zuzugreifen (Z1). Dieser Zugriff erfolgt in Form des Nur-Lesezugriffs unter Nutzung der beim Steuerpflichtigen eingesetzten Software und der darin vorhandenen Auswertungsmöglichkeiten. Beim unmittelbaren Datenzugriff nutzt der Betriebsprüfer das Datenverarbeitungssystem des Steuerpflichtigen in Form des Nur-Zugriffs, indem er Einsicht in die gespeicherten Daten nimmt und die vom Steuerpflichtigen oder von einem beauftragten Dritten eingesetzte Hard- und Software zur Prüfung der gespeicherten Daten einschließlich der Stammdaten und Verknüpfungen nutzt. Der Nur-Lesezugriff umfasst das Lesen, Filtern und Sortieren der Daten ggf. unter Nutzung der im Datenverarbeitungssystem vorhandenen Auswertungsmöglichkeiten.
Enthalten elektronisch gespeicherte Datenbestände andere, z.B. steuerlich nicht relevante personenbezogene oder dem Berufsgeheimnis i.S. des § 102 AO unterliegende Daten, so obliegt es dem Steuerpflichtigen oder dem von ihm beauftragten Dritten, durch geeignete Zugriffsbeschränkungen sicherzustellen, dass der Prüfer nur auf steuerlich relevante Daten des Steuerpflichtigen zugreifen kann.

4.2. Mittelbarer Datenzugriff (Z2)

Beim „mittelbarer Datenzugriff" – auch Z2 genannt – muss der Steuerpflichtige die Daten entsprechend den Vorgaben des Prüfers maschinell auswerten oder von einem Dritten auswerten lassen, damit anschließend ein „Nur-Lesezugriff" der Finanzverwaltung durchgeführt werden kann. Neben der Zurverfügungstellung von Hard- und Software gehört die Unterstützung des Prüfers durch Personen, die mit dem Datenverarbeitungssystem vertraut sind, zu den zu erfüllenden Anforderungen.

Ausartungen, die bestimmte Sortier- oder Selektionsfunktionen voraussetzen, die aber vom jeweiligen Softwareprogramm nicht abgedeckt werden, brauchen vom Steuerpflichtigen auch nicht geschaffen zu werden. Das bedeutet, dass der Prüfer nicht verlangen kann, speziell für ihn Auswertungstools anzuschaffen. Allerdings ist der Steuerpflichtige verpflichtet, dem Prüfer ggf. „technische" Unterstützung seitens eines mit dem DV-System vertrauten Mitarbeiters zu gewähren.

4.3. Datenträgerüberlassung (Z3)

Neben den beiden Zugriffsmöglichkeiten Z1 und Z2 steht dem Prüfer als dritte Alternative – Z3 – des Datenzugriffs die Datenträgerüberlassung der aufzeichnungs- und aufbewahrungspflichtigen Daten, einschließlich der jeweiligen Meta-, Stamm- und Bewegungsdaten sowie der internen und externen Verknüpfungen zur Verfügung. Sofern sich der Prüfer für die Datenträgerüberlassung entscheidet, sind die für Prüfungszwecke relevanten Daten samt aller zur Auswertung notwendigen Informationen (wie z.B. Formatangaben, Datenstruktur, Felddefinitionen, Verknüpfungen) auf einem maschinell lesbaren und auswertbaren Datenträger zu übergeben. Dies gilt auch dann, wenn sich die Daten bei einem mit der Buchhaltung beauftragten Dritten (z.B. Steuerberater, DATEV) befinden. Die Finanzbehörde ist nicht berechtigt, selbst Daten aus dem DV-System herunterzuladen oder Kopien vorhandener Datensicherungen vorzunehmen.

Die Datenträgerüberlassung umfasst auch die Mitnahme der Daten aus der Sphäre des Steuerpflichtigen, d.h., der Prüfer kann den Datenträger mit zur Amtsstelle nehmen.

Die Datenträger sind zurückzugeben bzw. zu löschen, sobald die Außenprüfung abgeschlossen ist und keine Einwände gegen die Prüfungsfeststellungen bestehen, spätestens aber nach Bestandkraft der aufgrund der Außenprüfung ergangenen Steuerbescheide.

*✐ **Hinweis:** Dem Prüfer sollen nur verschlüsselte Datenträger (mit separatem Passwort) ausgehändigt werden, da sonst das Risiko des Datenverlusts bzw. -missbrauchs beim Steuerpflichtigen liegt.*

5. Lösung (10 Punkte)

Durch den Einsatz von internetbasierten Kommunikationstechnologien, die Erweiterung des Kreises der möglichen Geschäftspartner sowie die Beeinflussung durch Dritte z.B. ISP oder anderer in der Geschäftsabwicklung ergeben sich E-Commerce spezifische Probleme und Risiken. Bei deren Analyse und Wertung kann unterschieden werden zwischen den Risiken, die sich aus der Kommunikation, und den Risiken, die sich aus der Verarbeitung ergeben.

- Risiken aus der Kommunikation

Die Kommunikation über öffentlich zugängliche Netzwerke beginnt ab dem Punkt, an dem der Absender bewusst die Einwirkungsmöglichkeit über die zu übermittelnden Daten (bspw. Transaktionsdaten) verliert, bis zu dem Punkt, an dem diese Daten dem Empfänger zugehen.

- Daten werden häufig ohne oder mit unzureichendem Schutz vor Verfälschung übertragen, was zu Integritätsverletzungen führen kann (Verlust der Integrität).
- Daten werden häufig unverschlüsselt oder unter Verwendung einer unsicheren Verschlüsselung übertragen, was eine Gefährdung der Vertraulichkeit bedeutet (Verlust der Vertraulichkeit).
- Der Anschluss eines IT-Systems an das Internet birgt die Gefahr, Ziel von Angriffen zu werden, bspw. durch Viren, Trojanische Pferde oder Hacker, die zu einer Gefährdung der Verfügbarkeit des IT-Systems führen (Verlust der Verfügbarkeit).
- Es existieren keine wirksamen Authentisierungsmechanismen zwischen den im Internet angeschlossenen Rechnern, bzw. es ist leicht möglich, falsche Adressen (IP-Spoofing) oder Rechnernamen (DNS-Spoofing) zu verwenden (Verlust der Authentizität).
- Beim Datentransfer können Hilfsprogramme (Java, Active-X) zu unautorisierten Zugriffen auf IT-Systeme führen (Verlust der Autorisierung).

- Risiken aus der Verarbeitung

Die Verarbeitung der Transaktionsdaten in der E-Commerce-Anwendung reicht von dem Punkt des Zugangs bis zu dem Punkt, an dem die Daten vom Front-End (Zugangs-/Erfassungssysteme) an die Rechnungslegungssysteme (z.B. ERP-Systeme) übergeben werden. Die Risiken ergeben sich aus der Transaktionsdatenverarbeitung in der E-Commerce-Anwendung sowie

insbesondere aus der Konvertierung, Entschlüsselung und Formatierung von Daten in der Schnittstelle zu anderen Teilen des IT-Systems.
Zu den Risiken bei der Verarbeitung führen insbesondere folgende Sachverhalte:

- Integritätsverletzungen bei Daten führen dazu, dass aufzeichnungspflichtige Geschäftsvorfälle nicht oder unvollständig erfasst werden (Verletzung des Vollständigkeitsgrundsatzes).
- Mangelnde Authentizität und Autorisierung bewirkt, dass Geschäftsvorfälle inhaltlich unzutreffend abgebildet werden (Verletzung des Grundsatzes der Richtigkeit).
- Störungen der Verfügbarkeit des E-Commerce-Systems und eine unzureichende Protokollierung des Datenverkehrs können eine zeitgerechte Aufzeichnung des Geschäftsvorfalls beeinträchtigen (Verletzung des Grundsatzes der Zeitgerechtigkeit).
- Eine unzureichende Aufzeichnung der eingehenden Daten kann zu einer Beeinträchtigung der Nachvollziehbarkeit der Buchführung (Verletzung des Grundsatzes der Nachvollziehbarkeit) und zu einem Verstoß gegen die Aufbewahrungspflichten
  (§ 257 HGB) führen.

6. Lösung (10 Punkte)

Gemäß Rz. 151 der „Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD)“ vom 28.11.2019 muss jedes Unternehmen eine **geschlossene Verfahrensdokumentation** (VFD) erstellen, aus der Inhalt, Aufbau, Ablauf und Ergebnisse des DV-Verfahrens vollständig und schlüssig ersichtlich sind.

Die konkrete Ausgestaltung der Verfahrensdokumentation ist abhängig von der Komplexität des eingesetzten DV-Systems und diese regelmäßig von der **Komplexität** und der **Diversifikation** der Geschäftstätigkeit sowie der Organisationsstruktur.
Die Verfahrensdokumentation soll den **organisatorisch und technisch gewollten Prozess** darstellen und reicht bei EDV-gestützten Verfahren von der Entstehung der Informationen über die Indizierung, Verarbeitung und Speicherung, bis hin zum eindeutigen Wiederfinden und der maschinellen Auswertbarkeit, der Absicherung gegen Verlust und Verfälschung und der Reproduktion.
Ziel der Anforderungen einer Verfahrensdokumentation ist es vorrangig, der Außenprüfung ein ausreichendes Verständnis der eingesetzten EDV-Anwendungen zu verschaffen und den Zugriff für die Prüfungen zu sichern.

Die Verfahrensdokumentation besteht in der Regel aus einer allgemeinen Beschreibung, einer Anwenderdokumentation, einer technischen Systemdokumentation und einer Betriebsdokumentation.
Für den Zeitraum der Aufbewahrungsfrist ist zu gewährleisten, dass das beschriebene Verfahren dem in der Praxis eingesetzten Verfahren entspricht.
Im Einzelnen sind folgende Bestandteile zu nennen:

- Anwender- und Systemdokumentation,
- internes Kontroll- und Steuerungssystem,
- umfassende Verfahrensdokumentation der organisatorischen und technischen Prozesse im Unternehmen,
- Belegfluss und Belegdigitalisierung,
- IT-Betriebsdokumentation.

7. Lösung (5 Punkte)

Art. 4 Nr. 1 DSGVO als Legaldefinition für personenbezogene Daten geht von einem weiten Verständnis personenbezogenen Daten aus und bezieht ausdrücklich alle Informationen mit Personenbezug in den Schutzbereich ein. Die Informationen können in jedem denkbaren Format vorliegen und auf beliebigen Datenträgern gespeichert sein.

Zu den typischen personenbezogenen Daten zählen neben dem Namen und der Anschrift einer Person:

- die Telefonnummer,
- die Kreditkarten- oder Personalnummer einer Person,
- die Kontodaten,
- ein Kfz-Kennzeichen,
- die Kundennummer,
- E-Mail-Adressen,
- die IP-Adresse.

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt (Art. 9 Abs. 1 DSGVO).

8. Lösung (6 Punkte)

Nach Art. 17 Abs. 1 DSGVO sind personenbezogene Daten unverzüglich zu löschen, wenn:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig (Zweckwegfall).
- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet (Rechtswidrigkeit der Datenverarbeitung).
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben.

Die betroffenen Daten sind unverzüglich zu löschen, das bedeutet **„ohne schuldhaftes Zögern"**.
Besteht die Löschungspflicht, so sind alle Empfänger von Daten über die Löschung zu informieren (Art. 19 DSGVO). Die Datenschutz-Grundverordnung normiert damit auch eine umfassende Mitteilungspflicht. Zusätzlich erlegt die DSGVO dem Verantwortlichen die Pflicht auf, andere Verantwortliche, denen die Daten zugänglich gemacht wurden, über den Antrag auf Datenlöschung zu benachrichtigen.

9. Lösung (3 Punkte)

Cloud Computing (deutsch Rechnerwolke oder Datenwolke) ist eine IT-Infrastruktur, die beispielsweise über das Internet verfügbar gemacht wird. Sie beinhaltet in der Regel Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung.

Technischer formuliert umschreibt Cloud Computing den Ansatz, IT-Infrastrukturen über ein Rechnernetz zur Verfügung zu stellen, ohne dass diese auf dem lokalen Rechner installiert sein müssen.

10. Lösung (5 Punkte)

CSV, xml, txt, xls, pdf

- csv

Das Dateiformat CSV steht für englisch Comma-separated values (seltener Character-separated values) und beschreibt den Aufbau einer Textdatei zur Speicherung oder zum Austausch einfach strukturierter Daten.

- xml

Die Extensible Markup Language (dt. „Erweiterbare Auszeichnungssprache“), abgekürzt XML, ist eine Auszeichnungssprache zur Darstellung hierarchisch strukturierter Daten im Format einer Textdatei, die sowohl von Menschen als auch von Maschinen lesbar ist.

- txt

Als Textdatei wird in der Informationstechnik eine Datei bezeichnet, die darstellbare Zeichen enthält. Der bei Textdateien physisch binär vorliegende Inhalt wird nach einer für die jeweilige Datei fest vorgegebenen Regel in Text umgewandelt.

- xls

„xls“ oder „xlsx“ ist das Dateiformat des am weitesten verbreiteten Tabellenkalkulationsprogramms Microsoft Excel. Neben den eigentlichen Funktionen können mit Excel sehr flexibel Daten eingelesen werden.

- PDF

Das Portable Document Format (englisch; kurz PDF; deutsch: (trans)portables Dokumentenformat) ist ein plattformunabhängiges Dateiformat. PDF-Dokumente können auf allen Computern geöffnet werden. Ein PDF-Dokument kann aus Texten und Bildern entstehen. Gleichzeitig wird in dem PDF-Dokument das Layout beibehalten, das der Urheber beim Erstellen verwendet hat. Dadurch sieht das PDF auf jedem Computer-System gleich aus.

11. Lösung (3 Punke)

Grundlage der Interpretation von Belegbildern ist die Texterkennung basierend auf optischer Zeichenerkennung (englisch: „optical character recognition“, abgekürzt: „OCR“). Es bezeichnet die automatisierte Texterkennung innerhalb von Bildern.

Als Ergebnis stehen aus den Belegbildern erzeugte, rohe Daten und Informationen bereit, die zur weiteren Verarbeitung aufbereitet werden müssen.

Aufgaben Teil 2:

1. Sachverhalt-Lösung (15 Punkte)

(allgemeintypisch und Software-System-unabhängig):
Die E-Mail ist im Dokumentenmanagementsystem als digitaler Posteingang zu erfassen. Dabei sind die vom System verlangten Angaben zum Absender, dem Zustellungsdatum und der Dokumentenart zu machen sowie die Zuordnung des zuständigen Erledigers anzugeben; ggf. ist das Dokument einem weiteren Mitarbeiter zur Kenntnisnahme zuzuordnen.
Die an die E-Mail angehängte Datei ist gesondert im Fristenkontrollsystem erfasst.

Folgende Angaben sind mindestens zu erfassen:
1. Eingangsdatum
2. Mandant
3. Dokumentenart (Bescheid, Brief, etc.)
4. Eingangsart (einfacher Brief, Zustellurkunde, etc.)
5. Steuerart
6. Veranlagungsjahr
7. Merkmale
8. Absender (Mandant, Finanzamt, etc.)
9. Zuständigkeit für den Posteingang
10. Fristentyp (Rechtsbehelfsfrist nach § 355 AO, Deutschland)
11. Bekanntgabe bei der Poststelle oder Bekanntgabe beim Mandanten
12. Zuständigkeit für die Bearbeitung des Dokuments
13. Dokumentendatum
14. Bekanntgabe-Datum
15. 1. Vorfrist (zur Kontrolle der Bearbeitung)
16. Fristende (Ende der Rechtsbehelfsfrist)
17. Bearbeitungsstand (offen, Einspruch, etc.)

Die eingehende E-Mail wird im Outlook-Archiv unter der zugeordneten unverschlüsselten Mandantennummer abgelegt.

Je nach System löst die Outlook-Archivierung die Verbindung zum Dokumentenmanagement-System der Kanzlei direkt aus. Dadurch wird die E-Mail innerhalb des berufsspezifischen Dokumentenablagesystems im Ablagefach des Mandanten abgelegt.

Mit der Ablage ist eine „Aufgabe" auszulösen, die die Aufgabe beschreibt, den / die verantwortliche/-n Mitarbeiter/-in benennt, den Beginn der Aufgabe, den Zeitpunkt für eine
1. Erinnerung und das Fristende benennt sowie den Status (begonnen, nicht begonnen, ...) und Grad der Bearbeitung (0% - 100%) angibt.

Die verantwortliche Person ruf den Bescheid aus seinem Ablageort zur Prüfung auf.
Die zu prüfenden Besteuerungsmerkmale werden mit einem Stempel (z. B. grüner Haken, rotes „x") gekennzeichnet; Abweichungen und Bemerkungen werden in einem Freitextfeld, das der jeweiligen Position angefügt wird, erfasst.

Nach Erledigung aller Prüfungsschritte wird auf dem Bescheid ein digitaler Stempel „geprüft am TT.MM.JJJ / Uhrzeit) angebracht; im Falle eines Rechtsbehelfs wird auf dem Bescheid ein weiterer digitaler Stempel „Rechtsbehelf / Einspruch / Widerspruch" aufgebracht.
Sollte ein Rechtsbehelf eingelegt werden, ist der Schriftsatz mit dem geprüften Bescheid zu verknüpfen (z. B. in einer elektronischen „Vorgangsmappe").

Anschließend wird ein Dokument (WORD, E-Mail) erstellt, mit dem der Mandant über das Prüfungsergebnis unterrichtet wird. Dieses Dokument wird ebenfalls mit dem geprüften Bescheid verknüpft und in die Vorgangsmappe eingestellt.

Der geprüfte und mit Stempelaufdrucken versehene Bescheid wird wieder an seinem bisherigen Ablageort mit Darstellung der Bearbeitungshistorie eingestellt.

Das Dokument mit dem Prüfergebnis wird in den elektronischen Postausgang übergeben und versandfertig gemacht oder direkt durch die zuständige Person per ……versandt. Erfolgt die Mitteilung per E-Mail, hat der E-Mail-Versand verschlüsselt zu erfolgen.

Ist ein Rechtsbehelf einzulegen, nutzt die zuständige Person die Schnittstelle zur Finanzverwaltung, erstellt dort den elektronischen Einspruch und übermittelt den entstandenen Datensatz an die Finanzverwaltung.

In der Vorauszahlungsdatei des Mandanten stellt die zuständige Person die künftig fälligen Vorauszahlungen auf die einzelnen Steuerarten ein.

Der Papier-Bescheid wird mit einem „Geprüft"-Stempel versehen und per Post an den Mandanten zurückgeschickt. Der analoge Postausgang ist im elektronischen Postausgang zu erfassen.

Die bei der Bearbeitung des Vorgangs angefallene Zeit wird im Zeiterfassungsprogramm eingegeben.

Wird ein Rechtsbehelf eingelegt, ist der Gegenstandswert für die Gebührenrechnung zu ermitteln und ebenfalls im Zeiterfassungssystem zu erfassen.
Die erfasste Zeit und ggf. ein Gegenstandswert werden an das Rechnungsschreibungssystem via Schnittstelle zur Erstellung der Gebührenrechnung übergeben.

<u>Beispiel bei Ver-/Anwendung von berufsspezifischer Anwendersoftware DATEV</u>

E-Mail	Microsoft Outlook
Posteingangserfassung	DATEV Post, Fristen und Bescheide / DATEV-Dokumentenmanagementsystem / E-Mail-Archivierung bei Verwendung des Dokumentenkorbs
Bescheid Erfassung Fristenerfassung	DATEV Fristen und Bescheide / Post- und
Bescheid-Prüfung	DATEV Fristen und Bescheide / Bescheid Prüfung
Elektronsicher -Rechtsbehelf	DATEV Einkommensteuer / Kommunikation mit der Finanzverwaltung
Vorauszahlungen Beitragszahlungen	DATEV Fristen und Bescheide / Steuer- und
Ergebnismitteilung	Microsoft Outlook
Bescheid Rückgabe	DATEV DMS / Dokument erstellen / DATEV DMS / Postausgang

Zeit-/ Gegenstands- -werterfassung	DATEV Zeiten und Kosten, Stoppuhr und Gegenstandswerte
E-Mail-Verschlüsselung	

2. Sachverhalt-Lösung (15 Punkte)

(allgemeintypisch und Software-System-unabhängig):

Die E-Mail geht verschlüsselt auf dem E-Mail-Account der Kanzleimitarbeiterin ein. Die E-Mail ist als Posteingang von der Mitarbeiterin im Dokumentenmanagementsystem der Kanzlei zu erfassen.

Die zu erfassenden Angaben sind (mindestens, systemabhängig)

- Tag des Eingangs,
- Art des Eingangs (E-Mail),
- Mitarbeiter, der für die Erledigung des Mandantenauftrags zuständig ist,
- ggf. eine weitere Person „zur Kenntnisnahme“,
- Kennzeichnung der Steuerrelevanz, ggf. Zuweisung zur „Handakte“ (Haken ja / nein),
- Die E-Mail ist im Dokumentenmanagement „unverschlüsselt“ abzuspeichern.

Der als Dateianhang beigefügte Beleg ist gesondert zu erfassen. Je nach Rechnungswesens -system ist der Beleg in eine Dateiablage einzustellen, aus der heraus der Beleg mittels OCR-Erkennung mit der Buchung verknüpft wird.

Beispiel bei Ver-/ Anwendung von berufsspezifischer Anwendersoftware DATEV

E-Mail	Microsoft Outlook
Posteingangserfassung	DATEV Post, Fristen und Bescheide / DATEV-Dokumentenmanagementsystem / E-Mail-Archivierung bei Verwendung des Dokumentenkorbs
Belegerfassung	Bei Verwendung des Dokumentenkorbs: Belegerfassung mit Angaben zum Mandat, dem Buchungsjahr und -monat und der Verarbeitungsart (z. B. „RE“ für Rechnungseingang
Zeit- / Gegenstands- -werterfassung	DATEV Zeiten und Kosten, Stoppuhr und Gegenstandswerte