Information

zu den

Datenverarbeitungen iSd

EU Datenschutz-Grundverordnung (DSGVO)

Version von 2024-04-27

Inhaltsverzeichnis

1 Vorbemerkungen **1**
1.1 Zweck und (Nicht-)Ziele . . . 1

2 Informationen **3**
2.1 Art. 4 . . . 3
2.2 Art. 5 . . . 3
2.2.1 Rechtmäßigkeit . . . 4
2.2.2 Verarbeitung nach Treu und Glaube, Richtigkeit . . . 4
2.2.3 Transparenz . . . 4
2.2.4 Zweckbindung und Datenminimierung . . . 4
2.2.5 Speicherbegrenzung . . . 4
2.3 Art. 6 . . . 5
2.4 Art. 9 . . . 6
2.5 Art. 13 . . . 6
2.5.1 Abs. 1 . . . 7
2.5.2 Abs. 2 . . . 8
2.5.3 Abs. 3 . . . 11
2.6 Art. 14 . . . 11
2.7 Art. 17 . . . 12
2.8 Art. 18 . . . 12
2.8.1 Abs. 2 . . . 12
2.9 Art. 24 . . . 12
2.10 Art. 25 . . . 12
2.10.1 Security by Design . . . 12
2.10.2 Security by Default . . . 13
2.11 Art. 30 . . . 13
2.11.1 Zwecke der Verarbeitung . . . 14
2.11.2 Datenkategorien . . . 14
2.11.3 Empfänger . . . 14
2.11.4 Dauer der Datenaufbewahrung . . . 14
2.12 Rechnungswesen (SA001) . . . 14
2.12.1 Zweck der Datenverarbeitung . . . 15
2.12.2 Datenverarbeitung . . . 15
2.13 Personalverrechnung (SA002) . . . 15
2.13.1 Zweck der Datenverarbeitung . . . 15
2.14 Datenverarbeitung . . . 15
2.15 Verwaltung (SA022) . . . 15
2.15.1 Zweck der Datenverarbeitung . . . 16
2.16 Datenverarbeitung . . . 16
2.17 Geldwäsche (SA037) . . . 16

2.17.1 Zweck der Datenverarbeitung 16
2.17.2 Dauer der Datenaufbewahrung 17
2.17.3 Empfänger 18
2.17.4 Datenverarbeitung 18
2.18 WiEReG 18
2.18.1 Zweck der Datenverarbeitung 18
2.18.2 Strafbestimmungen 19
2.18.3 Dauer der Datenaufbewahrung 19
2.18.4 Empfänger 20
2.18.5 Datenverarbeitung 20
2.19 Art. 32 20
2.19.1 Abs. 1 lit. c 20
2.20 Art. 33 21
2.21 Art. 34 21
2.22 Art. 35 21
2.23 Art. 37 21
2.24 Art. 40 22
2.25 Art. 44 22
2.26 Art. 88 22

A Tabellen **23**

Literatur **27**

Versionshistorie **29**

Kapitel 1

Vorbemerkungen

Am 25. Mai 2018 wurde das Datenschutzgesetz 2000 (DSG 2000) durch die EU-DSGVO (Datenschutz-Grundverordnung) abgelöst. Als EU-Verordnung ist diese unmittelbar - d.h. ohne Umsetzung in nationales Recht - anzuwenden. Die Rechtmäßigkeit der Verarbeitung nach den Bestimmungen des DSG 2000 ergab sich u.a. aus den Standardanwendungen, die in der Liste, im Anhang 1[1] der StMV 2004[2] (Standard- und Muster-Verordnung), aufgelistet waren.

Die Artikelbezeichnungen beziehen sich - wenn nichts anderes vermerkt ist - auf die DSGVO. Verweise auf das Bilanzbuchhaltungsberufegesetzt (BiBuG) 2014 beziehen sich auf die Fassung des BGBl. I 232 / 2022.

BiBuG Berufsberechtigte unterliegen nach den Bestimmungen des § 39 BiBuG einer strengen Verschwiegenheitsverpflichtung, die auch nach dem Ende des Auftragsverhältnisses mit dem Kunden weitergilt. Diese Verschwiegenheitspflicht löst in anderen Materiegesetzen ein Zeugnisentschlagungsrecht (Abs. 3) aus, wobei dieses iSd Abs. 1 als Pflicht zu verstehen ist - ausgenommen es kommt Abs. 4 zur Anwendung.

Die Berufsrechte dürfen erst nach der öffentlichen Bestellung durch die Aufsichtsbehörde ausgeübt werden (§§ 6 ff BiBuG). Das Register ist öffentlich einsehbar.

1.1 Zweck und (Nicht-)Ziele

Dieses Dokument stellt die zu veröffentlichenden Informationen an (mögliche) betroffene Personen zur Verfügung. Hier sind sowohl direkt betroffene Personen[3] als auch jene Personen adressiert, deren Daten zu verarbeiten sind, die nicht direkt bei der betroffenen Person erhoben werden (können). Die Verarbeitung der Daten kann sich aus (vor)vertraglichen Pflichten ergeben oder gesetzlich angeordnet sein.

Zu den deklarierten Nicht-Zielen dieses Dokumentes gehört die Offenlegung von internen Abläufen sowie von Betriebs- und Geschäftsgeheimnissen[4].

[1] Nicht meldepflichtige Standardanwendungen.
[2] BGBl II 312 / 2004, außer Kraft getreten am 24. Mai 2018.
[3] Bei denen Daten direkt erhoben werden.
[4] Siehe Art. 30 Abs. 2 lit. d DSGVO.

Kapitel 2

Informationen

2.1 Art. 4

Nach der Legaldefinition der Z. 7 entscheidet ein Verantwortlicher über die Mittel und Zwecke der Datenverarbeitung alleine oder gemeinsam mit einem anderen Verantwortlichen.

§ 33 Abs. 1 BiBuG verpflichtet Berufsberechtigte, Ihren Beruf gewissenhaft, sorgfältig, eigenverantwortlich und unabhängig auszuüben.

§ 36 Abs. 1 BiBuG verpflichtet Berufsberechtigte Aufträge abzulehnen, bei denen sie an fachliche Weisungen des Auftraggebers gebunden wären. § 4 Abs. 4 der Berufsausübungsrichtlinie (BB-AR 2014) verlangt die Zurücklegung eines Auftrages, wenn sich nachträglich die Unerfüllbarkeit des verlangten Verhaltens herausstellen sollte.

Da ein Auftragsverarbeiter (iSd Legaldefinition der Z. 8) gemäß Art. 28 Abs. 3 Z. a nur bei Vorliegen einer dokumentierten Weisung des auftraggebenden Verantwortlichen eine Datenverarbeitung durchführen darf, ist für die BhB nur die Einordnung als Verantwortlicher iSd der Legaldefinition der Z. 7 in zulässig.

2.2 Art. 5

Artikel 5 hat die Überschrift "Grundsätze für die Verarbeitung personenbezogener Daten". Auf die genannten Grundsätze

- Rechtmäßigkeit
- Verarbeitung nach Treu und Glaube
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit

- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

wird, soweit nötig, im Folgenden eingegangen.

2.2.1 Rechtmäßigkeit

Diese ergibt sich insbesonders aus den gesetzlich auferlegten Pflichten, die für Abgabepflichtige gelten. Darüberhinaus kommen vorvertragliche Pflichten zur Anwendung, die sich speziell aus der nationalen Umsetzung der EU-Geldwäsche-RL ergeben - siehe Kap. 2.17.

2.2.2 Verarbeitung nach Treu und Glaube, Richtigkeit

Nach § 36 Abs. 3 BiBuG dürfen die vom Kunden erhaltenen Daten und Auskünfte als richtig und vollständig angesehen werden.

2.2.3 Transparenz

Das Gebot der Transparenz kann nur für den unmittelbaren Kunden gelten. Anderfalls wäre die Verschwiegenheitspflicht des § 39 BiBuG verletzt - sofern dem nicht eine gesetzliche Offenlegungspflicht entgegensteht.

2.2.4 Zweckbindung und Datenminimierung

Es werden nur so viele Daten erhoben und verarbeitet, wie zur Erfüllung der vorvertraglichen Pflichten bzw. für die Erfüllung des laufenden Auftrages benötigt werden.

2.2.5 Speicherbegrenzung

Berufsberechtigte haben insbesonders gemäß den nachfolgenden gesetzlichen Bestimmungen die verarbeiteten Daten aufzubewahren[1]:

- gemäß § 132 BAO für die Dauern von 7 Jahren - die Frist beginnt mit Ablauf des Kalenderjahres zu laufen;
- gemäß § 207 BAO für eine Dauer von 10 Jahren ab dem Ende des Kalenderjahres, in dem die Abgabenverkürzung beendet wurde. Mit § 209 BAO verlängert sich diese Frist, wenn nach außen erkennbare Amtshandlungen zur Geltendmachung unternommen werden, um deren Dauer;

[1] Siehe auch § 5 in 2.

- gemäß § 11 Abs. 2 UStG letzter Satz für die Dauer von 7 Jahren;
- gemäß § 18 Abs. 10 UStG für eine Dauer von 12 Jahren (bei Grundstücksumsätzen);
- gemäß § 212 UGB für eine Dauer von 7 Jahren, ab dem Ende des Kalenderjahres;
- gemäß § 41a ASVG kommen die Aufbewahrungsfristen der BAO zur Anwendung;
- gemäß Gleichbehandlungsgesetz für eine Dauer von 7 Monaten, für die mögliche Abwehr eines Schadenersatzbegehrens wegen (behaupteter) Diskriminierung;
- die nationale Umsetzung der EU-Geldwäsche-RL im BiBuG bzw. im WiEReG normiert eine generelle Aufbewahrungspflicht von 5 Jahren. § 52c Abs. 1 BiBuG normiert eine mindestens 5-jährige Aufbewahrungsdauer nach dem letzten Geschäftsfall.

Während einer Außenprüfung nach den Bestimmungen der §§ 147 ff BAO ist der Fristenlauf gehemmt. Ebenso während der Ausschöpfung von Rechtsmitteln gegen ergangene Bescheide iSd § 92 BAO.

Die Frist zum Ablauf der Aufbewahrungspflicht wird auch gehemmt, solange ein behördliches oder gerichtliches Verfahren droht oder bereits anhängig ist, in dem die verarbeiteten Daten benötigt werden könnten.

Wie lange die Daten zu speichern sind, ist daher eine Einzelfallentscheidung, die von der Gesamtheit der Umstände abhängig ist. Diese Entscheidung kann nur ex ante getroffen werden.

Nach Ablauf der gesetzlich determinierten Aufbewahrungsfrist wird, anhand des implementierten Löschkonzeptes - welches als Betriebs- und Geschäftsgeheimnis klassifiziert ist, und somit an anderer Stelle dokumentiert ist - die Löschung von Daten durchgeführt, deren Aufbewahrungsfrist abgelaufen ist.

2.3 Art. 6

Die "Rechtmäßigkeit der Verarbeitung" der zu verarbeitenden Daten iSd Abs. 1 lit. a bis f ergibt sich einerseits durch den erteilten Auftrag vom Kunden und andererseits durch rechtliche Vorgaben. Diese ergeben sich vor allem aus Pflichten zum Führen von Aufzeichnungen, die beispielsweise im Abgabenrecht, im Arbeitsrecht sowie im Sozialversicherungsrecht definiert sind.

Durch die Begründung eines Vertragsverhältnisses mit einem Kunden, sind dessen persönliche Daten, als abgabenpflichtige Person, zu verarbeiten (lit. a).

Lit. b kommt zur Anwendung, wenn vor Vertragsabschluß zu prüfen ist, ob in Bezug auf die Bestimmungen der EU-Richtlinie zur Vermeidung von Geldwäsche und Terrorismusfinanzierung[2] die vereinfachte Prüfung angewandt werden darf

[2] siehe Art. 41 und Art. 43 der RL 849/2015/EU

oder ob die erhöhten Sorgfaltspflichten anzuwenden sind. § 46 BiBuG schreibt jene Daten vor, die vor dem Eingehen der Geschäftsbeziehung einzuholen sind - siehe auch Kap. 2.17.

In sinngemäßer Anwendung des Urteils DSB-D123.589/0002-DSB/2019 vom 9. April 2019 der Datenschutzbehörde erlaubt Abs. 1 lit. b bei einem aufrechten Vertragsverhältnis die Verarbeitung der Daten der Dienstnehmer, der Kunden und der Lieferanten des Kunden, um dieses erfüllen zu können.

Die lit. c, e und f werden über die bereits oben erwähnten rechtlichen Pflichten, Daten für die Zwecke der Abgabenerhebung zu erfassen, erfüllt. Zusätzlich kommen die Verpflichtungen zur Archivierung der Daten - neben den im Kapitel 2.2.5 genannten - noch beispielsweise folgenden Bestimmungen zur Anwendung: § 8 ArbIG, § 5 ASchG und § 26 AZG

Für das Sozialversicherungsrecht seien exemplarisch die §§ 33 ff ASVG angeführt. Damit werden die Grundsätze der *Rechtmäßigkeit* und der *Zweckbindung* des. Art. 5 erreicht.

Der gesetzliche Auftrag zur Verarbeitung von (personenbezogenen) Daten - iSd lit. e - hat starken Einfluß auf die Erfüllung der Art. 33 f. Das öffentliche Interesse der lit. e besteht beispielsweise in der gleichmäßigen Einhebung der Abgaben iSd § 114 Abs. 1 BAO.

2.4 Art. 9

Die "Verarbeitung besonderer Kategorien personenbezogener Daten" meint die sensiblen Daten iSd DSG 2000.

Auch bisher wurden keine Daten verarbeitet, aus denen die rassische oder ethnische Herkunft, die politische Meinung, die religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit ableitbar sind. Dies entspricht dem Grundsatz der *Datenminimierung* des Art. 5. Derartige Daten werden auch weiterhin nicht verarbeitet werden - in Übereinstimmung mit dem Grundsatz der *Speicherbegrenzung* des Art. 5.

Die Ausnahmen nach Abs. 2 lit. b bzw. lit. g, die eine Verarbeitung besonderer Kategorien erlauben, beziehen sich exemplarisch auf die Erfüllung des Abgabenrechtes oder auf arbeitsrechtliche Bestimmungen wie z.B. die Entgeltfortzahlung im Krankheitsfall. Für das Abgabenrecht sei exemplarisch die gesetzlich normierte Führung des Lohnkontos erwähnt.

Für die Ausnahme nach Abs. 2 lit. h sind exemplarisch die Schutzbestimmungen des MuSchG relevant.

2.5 Art. 13

Die "Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person" wird im Akquiseprozeß fällig, wenn Daten aufzunehmen sind, die nicht mehr öffentlich zugänglich sind.

Für die vorvertragliche Pflicht eine Risikoeinschätzung - iSd der nationalen Umsetzung in den §§ 43 ff BiBuG 2014 der EU Richtlinie zur Vermeidung von Geldwäsche und Terrorismusfinanzierung - vorzunehmen, kann bei aufrechten Unternehmern auf die öffentlich zugänglichen Daten zugegriffen werden. In diesem Fall kommt es zu keiner "Erhebung bei der betroffenen Person", weshalb diese Information unterbleiben darf[3]. Bei Gründern erfolgt diese Einschätzung beim (persönlichen) Erstgespräch. Die in Frage kommenden Datenkategorien und deren mögliche Empfänger sind im Kap. 2.17 bzw. 2.18 angeführt.

Sollte eine Vertragsbeziehung eingegangen werden, sind für die Erstellung der Vollmachten[4] Daten von der betroffenen Person zu erheben, die nicht mehr öffentlich zugänglich sind. Gem. Abs. 4 darf diese Information entfallen, wenn sie bereits bei der betroffenen Person vorhanden ist. Alternativ führt der Erw.Gr. 62 weitere Optionen an, bei denen diese Information entfallen kann[5].

§ 2 ABGB definiert das "Wissen müssen" im österreichischen Rechtsbestand. Der VwGH verlangt generell seit vielen Jahren in ständiger Judikatur von Unternehmern, sich aktiv über die einzuhaltenden Vorschriften zu erkundigen[6].

Da die durchzuführenden Datenverarbeitungen auf gesetzlichen Anordnungen oder Strafandrohungen[7] beruhen und die strenge Verschwiegenheitspflicht des § 39 BiBuG als "ausreichende Garantie" iSd Erw.Gr. 62 letzter Satz gewertet werden darf, könnte die Information nach diesem Artikel bei Unternehmern, die ihre Firma in der Rechtsform einer Gesellschaft betreiben, unterbleiben.

Die Daten eines (zukünftigen) Dienstnehmer sind solche, die nicht direkt von der betroffenen Person erhoben werden (können), weswegen in diesem Fall Art. 14 DSGVO anzuwenden ist.

Im Nachfolgenen wird auf die speziellen Informationspflichten eingegangen. Der Text in Anführungszeichen zitiert die dazugehörige Bestimmung der DSGVO.

2.5.1 Abs. 1

"Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:"

lit. a

"den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenfalls seines Vertreters;"

Wie auch u.a. im Code of Conduct[8] ausgeführt, kann die BhB nur als Verantwortlicher iSd Art. 24 DSGVO tätig werden. Die Kontaktdaten sind im Impressum öffentlich zugänglich.

[3] Vgl. Kap. 2.6 letzter Absatz.

[4] Siehe u.a. § 35 Abs. 3 ASVG oder § 83 BAO.

[5] U.a. wenn die Datenverarbeitung ausdrücklich durch Rechtsvorschriften geregelt ist oder die Erteilung dieser Information ist mit unverhältnismäßig hohem Aufwand verbunden.

[6] Den Begriff "Erkundigungspflicht" als Suchwort im RIS bei den VwGH-Judikaten verwendend, liefert mehrere Bildschirmseiten mit einschlägigen Judikaten.

[7] Stellvertretend seien nur die §§ 153c bis 153e StGB erwähnt.

[8] Siehe 2.

lit. b

”gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;”

Die Bestellung eines Datenschutzbeauftragten ist weder erforderlich noch ist dies erfolgt.

lit. c

”die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;”

Die Zwecke der Datenverarbeitung sind im Kap. 2.11 ausgeführt. Die Rechtsgrundlagen sind beispielsweise das Abgabenrecht, das SV-Recht oder das Arbeitsrecht. Die Verarbeitungen finden auf der Grundlage gesetzlicher Anordnungen statt. Eine weiterführende Auflistung ist in [2] enthalten.

Da sich die gesetzlichen Anforderungen an Abgabenpflichtige bzw. Dienstgeber laufend ändern, kann hier nur sehr allgemein darauf eingegangen werden. Gemäß der ständigen Judikatur des VwGH haben sich Unternehmer aktiv zu erkundigen, welche Pflichten sie zu erfüllen haben.

lit. e

”gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten”

Diese listet die Tabelle A.6 (exemplarisch) auf - vgl. Kap. 2.11 enthalten. Auch hier gilt die Erkundigungspflicht der normunterworfenen Unternehmers bez. der sich laufend ändernden gesetzlichen Vorgaben.

lit. f

”gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln”

Es besteht keinerlei Absicht die zu verarbeitenden Daten irgendwo anders hin zu übermitteln, als an die unbedingt notwendigen Empfänger. Zu den nach Art. 32 DSGVO zu treffenden Maßnahmen gehört u.a. die Verweigerung des Einsatzes von Cloud-Diensten.

2.5.2 Abs. 2

”Zusätzlich zu den Informationen gem. Abs. 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:”

lit. a

”die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;”

Wie lange die erhaltenen Daten aufzubewahren sind, ist - wie z.B. in [§ 5 2] angeführt - im Einzelfall nach der anzuwendenden gesetzlichen Bestimmung zu bewerten.

Die allgemeine abgabenrechtliche Mindestaufbewahrungsdauer beträgt 7 Jahre. Im Einzelfall kann diese Dauer - z.B. durch die gesetzliche Anordnung einer Fristenhemmung - auch wesentlich länger sein. Die tatsächlich anzuwendende Aufbewahrungsdauer kann nur im Einzelfall, nach Abwägung aller verfügbarer Informationen, bestimmt werden.

Ob die vom OGH judizierte absolute Verjährungsfrist von 30 Jahren[9] auch im Abgabenrecht anwendbar ist, bleibt abzuwarten.

Bez. der Aufbewahrung von Kundenbelegen - nach dem Ende der Vertragsbeziehung - behält sich die BhB deren Vernichtung nach Ablauf einer 10-jährigen Aufbewahrungsfrist vor.

lit. b

”das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie das Recht auf Datenübertragbarkeit;”

Das Recht auf Auskunft kann von berufsrechtlichen Vorgaben[10] eingeschränkt werden. Ebenso kann das Recht auf Auskunft eingeschränkt werden, wenn Berufs- bzw. Geschäftsgeheimnisse gefährdet wären[11]. Dies ist eine ex ante zu treffende Einzelfallentscheidung, auf Basis der vorliegenden Informationen.

Berichtigungen oder Löschung der Daten sind im Einzelfall gegen anzuwendende gesetzliche Anordnungen abzuwägen. Für die Übertragung der Daten bedarf es eines ausdrücklichen Kundenwunsches. Bezüglich des Rechtes auf Einschränkung der Verarbeitung ist auf den Status des Vertragsverhältnisses abzustellen, sowie die geltende Rechtslage zu beachten. Die Löschung der Daten darf erst nach Ablauf der bei der lit. a erwähnten Aufbewahrungsfrist erfolgen. Das dzugehörige Löschkonzept ist als Betriebs- und Geschäftsgeheimnis klassifiziert und dementsprechend an anderer Stelle dokumentiert.

lit. c

”wenn die Verarbeitung auf Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a beruht, das Bestehen eines Rechtes, die Einwilligung jederzeit widerrufen, ohne daß die Rechtmäßigkeit der aufgrund der Einwillung bis zum Widerruf erfolgten Verarbeitung berührt wird;”

[9] Im ABGB beginnt die 3 jährige Verjährungsfrist ab Kenntnis von Schaden und (kumulativ) des Schädigers. Lt. OGH Judikat endet sie absolut nach 30 Jahren, unabhängig davon ob die vorhin genannte Eintrittsbedingung in den Fristenlauf erfüllt ist.

[10] Hier sind speziell die §§ 39 und 52b BiBuG eingschlägig.

[11] § 4 Abs. 5 DSG 2018

Einem Widerruf der Einwilligung zur Datenverarbeitung entspricht das Beenden der Geschäftsbeziehung.

Solange die Geschäftsbeziehung aufrecht ist, sind Sie Abgabenpflichtiger bzw. Dienstgeber. In dieser Eigenschaft ist den gesetzlichen Aufträgen zur Verarbeitung aller nötigen Daten, um den jeweils normierten Pflichten entsprechen zu können, Folge zu leisten. Hierfür kommen die Bestimmungen des Art. 6 Abs. 1 lit. f[12] DSGVO sowie Art. 9 Abs. 2 lit. b[13] DSGVO zur Anwendung.

lit. d

"das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;"

Zur Möglichkeit der Beschwerde enthält [2] ausführliche Informationen. Bzw. direkt auf der Homepage der DSB.

lit. e

"ob die Bereitstellung der peronenbezogen Daten gesetzlich oder vertraglich vorgeschrieben oder für den Vertragsabschluß erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und"

Da die Datenverarbeitungen auf gesetzlichen Anordnungen beruhen, kann ein Vertragsverhältnis nur zustande kommen oder aufrecht erhalten werden, wenn die zur Erfüllung der gesetzlichen Abgabe- und Meldepflichten notwendigen (persönlichen) Daten mit ausreichender Vorlaufzeit und vollständig offen gelegt werden.

Dazu gehören u.a. Daten des Kunden, Daten seiner Kunden bzw. Lieferanten bzw. Daten seiner Dienstnehmer. Siehe auch Kap. 2.11.

Diese aktive Offenlegung darf als Einwilligung iSd Art. 6 Abs. 1 lit a bzw. Art. 9 Abs. 2 lit. a DSGVO verstanden werden.

lit. f

"das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gem. Art. 22 Abs. 1 und 4 und - zumindestens in diesen Fällen - aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person."

Diese Art der Verarbeitung findet nicht statt.

[12] Zu den berechtigen Interessen eines Dritten gehören u.a. die im § 144 BAO normierten Grundsätze.

[13] Hier sind die arbeitsrechtlichen Schutznormen angesprochen, die Dienstnehmern zugute kommen.

2.5.3 Abs. 3

"Beabsichtigt der Verantwortliche die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gem. Abs. 2 zur Verfügung."

Es bestehen keinerlei Absichten oder Intentionen, die erhaltenen Daten für andere Zwecke zu verarbeiten, als zur Erfüllung der gesetzlich angeordneten Offenlegungs- und Meldepflichten, die im Rahmen der Berufsrechte gem. BiBuG notwendig sind bzw. um die (vor)vertraglichen Vereinbarungen zu erfüllen.

2.6 Art. 14

Die "Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden" betrifft im Wesentlichen die Dienstnehmer des Kunden bzw. dessen Vertragspartner. Zum anderen entfällt gem. Abs. 5 diese Pflicht, wenn (lit. a) die betroffene Person bereits über die Information verfügt, dies einen unverhältnismäßig hohen Aufwand bedeutet (lit. b) oder (lit. d) die zu verarbeitenden Daten einem Berufsgeheimnis unterliegen und daher vertraulich zu behandeln sind.

§ 39 BiBuG verpflichtet jeden Berufsberechtigten zur Verschwiegenheit, die nach dem Ende des Vertragsverhältnisses fortdauert. Somit kann unter Anwendung des Abs. 5 lit. d diese zusätzliche Informationspflicht entfallen. Lit. a wäre erfüllt, wenn diese Information vom Kunden an seine Dienstnehmer erteilt wird. Subsidiär ist die lit. b anwendbar.

Mit der Verschwiegenheitspflicht des § 39 BiBuG wird der Grundsatz der *Vertraulichkeit* des Art. 5 erfüllt.

Weiters wäre die Erteilung dieser Information an jede indirekt betroffenen Person mit einem "unverhältnis hohen Aufwand" (iSd Abs. 5 lit. b) verbunden. In diesem Zusammenhang sei auch auf [§ 7 2] verwiesen.

Ergänzend sei erwähnt, daß die Erfüllung der Meldepflichten des § 33 Abs. 1 ASVG nur dann erfüllt werden kann, wenn der (zukünftige) Dienstnehmer jene Daten offenlegt, die für die Durchführung der Personalverrechnung[14] benötigt werden. Somit darf diese Information beim Dienstnehmer als bekannt (Abs. 5 lit. a) angenommen werden. Andernfalls dürfte der Dienstgeber die betroffene Person nicht in seinem Betrieb anstellen (dürfen).

Ebenso kann es durch die (berufsrechtlich angeordnete) Einsicht in öffentliche Register[15] zu einer indirekten Erhebung von personenbezogenen Daten kommen. Deren Offenlegung erfolgte auf Basis einer gesetzlichen Anordnung[16]. Diese Daten werden nur wenn notwendig verarbeitet. Mit dem oben gesagten darf die Information der Betroffenen entfallen.

[14] Nach den Bestimmungen des SV-Rechtes und des Abgabenrechtes.

[15] Dazu gehören insbesonders das GISA, das Firmenbuch und das Register der Wirtschaftlichen Eigentümer (siehe Kap. 2.18).

[16] Siehe Erw.Gr. 62 DSGVO.

2.7 Art. 17

Das ”Recht auf Löschung” gilt nicht, wenn Abs. 3 lit. b oder Abs. 3 lit. e zutrifft. Beide Bedingungen sind durch die Darstellung im Kapitel 2.2.5 zutreffend.

Technisch bedingt ist ein nach Abs. 1 zulässiges Löschen von Daten, die sich in einer Sicherungen befinden, die gemäß Art. 32 Abs. 1 lit. c (siehe Kapitel 2.19.1) anzulegen sind, nicht möglich. Hierzu sei auf Kapitel 2.8.1 verwiesen.

2.8 Art. 18

Die Beschränkung des ”Recht auf Einschränkung der Verarbeitung” nach Abs. 2 ist nötig, um der Verpflichtung auf rasche Wiederherstellung bei einem Zwischenfall (siehe Kapitel 2.19.1) nachkommen zu können.

2.8.1 Abs. 2

In Anwendung des § 4 Abs. 2 DSG 2018 werden Daten, für die die Löschung nach Art. 17 Abs. 1 zulässig ist, durch deren Überschreiben im Rahmen des Backup-Konzeptes (siehe Kapitel 2.19.1), gelöscht. Die Einschränkung der Verarbeitung ergibt sich aus der Tatsache, daß ein Sicherungsmedium (organisatorisch) der regulären Verarbeitung entzogen ist.

2.9 Art. 24

Die ”Verantwortung des für die Verarbeitung Verantwortlichen” umfaßt u.a. die beim Art. 25 beschriebenen technischen Maßnahmen bzw. die beim Art. 32 beschriebenen organisatorischen Maßnahmen.

2.10 Art. 25

Der ”Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen” wird - obwohl im Prinzip untrennbar, da beides einander bedingt - hier getrennt behandelt. Die weiterführenden Details, sowie die Ergebnisse der Risikoanlayse, sind als Betriebs- und Geschäftsgeheimnisse klassifiziert, und daher an anderer Stelle dokumentiert.

2.10.1 Security by Design

Zum Datenschutz durch Technikgestaltung gehört u.a. die Verwendung einer privaten Netzwerkadresse[17] für das Intranet. Zugriffe über das Internet - z.B. durch einen VPN-Tunnel - sind weder vorhanden noch geplant. Meldungen wie z.B. [10]

[17] Siehe 11.

sind eine (nachträgliche) Bestätigung für diese Designentscheidung. Die Verwendung von WLAN war schon vor dem Bekanntwerden der "KRACK-Attacke[18]" nicht möglich. Trotz der Beschreibung in [9] wird es dabei bleiben.

2.10.2 Security by Default

Zum Datenschutz durch datenschutzfreundliche Voreinstellungen muß festgehalten werden, daß Microsoft-Produkte "**in**secure by default" sind. Deswegen kommen wo immer möglich nur mehr Open-Source-Produkte zum Einsatz[19]. Durch legistische Maßnahmen, wie z.B. den US Patriot Act, der US Behörden vollen Zugriff auf alle Daten gewährt, die sich in einer "Cloud" befinden, wenn der Betreiber ein amerikanisches Unternehmen ist oder einen amerikanischen Eigentümer hat, verbietet den Einsatz jeder Art von Cloud-Lösung von selbst.

Die Microsoft-Konfiguration von Windows 10 gewährt vom Werk aus, jeder MS-App den Vollzugriff auf alle Daten - inklusive aktivierter Geo-Location, aktivierter Kamera-App und aktivierter Mikrofon-App. Während es bei Windows 7 noch vergleichsweise einfach war, die Konfiguration zu finden, um eine datenschutzfreundlichere Einstellung vornehmen zu können, wird mittlerweile bei Windows 10 diese Konfiguration so gut versteckt, daß man explizit wissen muß, mit welchem aufzurufenden Tool eine datenschutzfreundlichere Einstellung erreicht werden kann. Bei Windows 8 sind diese Einstellungen bereits besser versteckt als noch bei Windows 7, aber leichter erreichbar als bei Windows 10. Diesem Thema widmen sich u.a. [7] oder z.B. [1]. Allgemein ist ein DSGVO konformer Einsatz von Windows-Systemen faktisch unmöglich. Leider ist jede verfügbare beruflich relevante Software mit einem adäquaten Funktionsumfang nur unter Windows erhältlich.

2.11 Art. 30

Die Buchhaltung Blaschka GmbH ist Verantwortlicher iSd der Legaldefinition des Art. 4 Z. 7 DSGVO. Der für die Datenverarbeitung Verantwortliche ist der gewerberechtliche Geschäftsführer der Buchhaltung Blaschka GmbH. Der Name und die Kontaktdaten können entweder dem öffentlich einsehbaren Firmenbuch entnommen werden, oder dem Impressum. Mitarbeiter und gegebenenfalls Auftragnehmer unterliegen der Verschwiegenheitspflicht des § 39 BiBuG. Die Daten des beauftragenden Kunden, sowie die von diesem erhaltenen Daten, fallen unter die gesetzlich angeordnete Verschwiegenheitspflicht des § 39 BiBuG.

Soweit eine Datenübermittlung sich nicht schon aus einer definierten Verpflichtung ergibt oder im Rahmen der Auftragserfüllung durchzuführen ist, findet diese nur auf Wunsch des Kunden statt. Dies ist speziell beim Wechsel der betreuenden Kanzlei relevant. Eine Übermittlung in ein Drittland findet nur dann statt, wenn sich dies (implizit[20]) aus einer gesetzlichen Anordnung ergibt.

[18] Siehe 8.

[19] Für die Open Source Community hat Datensicherheit eine sehr hohe Priorität.

[20] Beispielsweise, weil der die Daten empfangende Auftragsverarbeiter in einem Drittland ansäßig ist.

Um den Auftrag des Art. 32 Abs. 1 lit. c DSGVO[21] erfüllen zu können, werden die Daten im Rahmen des erstellen Sicherungskonzeptes[22] auch in einem anderen Land innerhalb des EWR gesichert. Die eigentliche Verarbeitung im engeren Sinne, findet ausschließlich im Intranet auf selbst betriebener Hardware statt.

2.11.1 Zwecke der Verarbeitung

Die Tabelle A.1 enthält eine Übersicht zu den durchzuführenden Verarbeitungstätigkeiten, bzw. listet die Tabelle A.2 die in Frage kommenden Kategoriern betroffener Personen auf. Grundsätzlich erfolgt die Datenverarbeitung im Rahmen der gesetzlichen Verpflichtungen, die sich beispielsweise aus dem Abgabenrecht, dem Arbeitsrecht oder dem Sozialversicherungsrecht ergeben.

2.11.2 Datenkategorien

Mit jeder Novelle einer anzuwendenden gesetzlichen Bestimmung oder eines in der Personalverrechnung relevanten Kollektivvertrages können sich dadurch Änderungen in zu verarbeitenden Datenkategorien ergeben. Deswegen sind diese absichtlich allgemein gehalten, daß damit auch mögliche zukünftige Gesetzesänderungen abgedeckt werden können, ohne dieses Dokument bei jeder Novelle einer anzuwendenden gesetzlichen oder kollektivvertraglichen Norm von Grund auf überarbeiten zu müssen.

2.11.3 Empfänger

Die Tabelle A.3 listet die in die Frage kommenden Empfänger für eine Datenkategorie auf. Diese ist jedoch nicht taxativ zu lesen, sondern deklarativ, da sich mit jeder Gesetzesänderung auch eine Änderung der Empfänger ergeben kann. Bei den einzelnen Datenverarbeitungen werden deswegen die möglichen Empfänger für die jeweilige Datenkategorie auch nur deklarativ genannt. Die tatsächlichen Empfänger ergeben sich aus den anzwendenden gesetzlichen Normen.

2.11.4 Dauer der Datenaufbewahrung

Soweit im Nachfolgenden nichts anders angegeben wird, richtet sich diese nach den gesetzlichen Aufbewahrungsfristen. Siehe dazu § 5 Abs. 2 [2]. Die tatsächliche Aufbewahrungsdauer kann nur im Einzelfall, nach Abwägung aller verfügbaren Informationen, bestimmt werden. Das gemäß § 5 Abs. 5 [2] implementierte Löschkonzept ist als Betriebs- und Geschäftsgeheimnis klassifiziert und daher an anderer Stelle dokumentiert.

2.12 Rechnungswesen (SA001)

Diese Anwendung meint die Durchführung der Buchhaltung im Auftrag eines Kunden.

[21] "die Fähigkeit, die Verfügbarkeit ... rasch wieder herzustellen;"
[22] Siehe § 5 Abs. 6 in [2].

2.12.1 Zweck der Datenverarbeitung

Verarbeitung der erhaltenen Buchhaltungsdaten eines Kunden, inklusive der elektronisch erstellten Dokumente, sowie deren Archivierung, soweit diese elektronisch vorliegen. Übermittlung der Ergebnisse an den Kunden bzw. an Behörden, soweit dies gesetzlich vorgegeben ist. Speziell bei Bilanzierern sind hier auch die Daten von Kunden und Lieferanten des (eigentlichen) Kunden zu erfassen, soweit diese im Rahmen einer Geschäftsbeziehung offen gelegt werden müssen[23].

2.12.2 Datenverarbeitung

Siehe Tabelle A.4.

2.13 Personalverrechnung (SA002)

Diese Anwendung adressiert privatrechtliche Dienstverhältnisse des Kunden und ist daher auch für den Art. 88 DSGVO relevant.

2.13.1 Zweck der Datenverarbeitung

Erhalten, Verarbeiten, Übermitteln und Archivieren von Daten, die für die Einhaltung der Aufzeichnungs-, Auskunfts- und Meldepflichten benötigt werden. Speziell soweit dies auf Grund gesetzlicher Vorgaben oder durch die anzuwendenden Kollektivverträge erforderlich ist. Dazu gehört gegebenenfalls auch die Evidenzierung jener Daten, die für die Auftragserfüllung notwendig sind. Ebenfalls zu verarbeiten sind alle Daten, die benötigten werden, um den Bestimmungen des Arbeitsrechtes oder des Sozialversicherungswesen zu entsprechen. Z.B. im Falle der Entgeltfortzahlung im Krankheitsfall, sind damit auch besondere Kategorien[24] gemeint. In diesem Kontext können auch Daten von fremden Dritten zu erfassen sein, wie es beispielsweise bei einer Gehaltsexekution der Fall ist[25].

2.14 Datenverarbeitung

Siehe Tabelle A.5.

2.15 Verwaltung (SA022)

Die Anwendung "Kundenbetreuung und Büroautomation" ist grundsätzlich weit zu verstehen.

[23] Siehe Kap. 2.6 letzter Absatz.
[24] Im Sinne des Art. 9 DSGVO aka sensible Daten.
[25] Siehe Kap. 2.6 letzter Absatz.

2.15.1 Zweck der Datenverarbeitung

Die formale Behandlung zu besorgender Geschäfte, inklusive der Aufbewahrung der angefallenen sowie der erhaltenen Dokumente. Dazu gehören auch die erhaltenen und versandten Briefe bzw. der elektronisch geführten Kommunikation. Sowie all jener Daten, die für die Fakturierung der erbrachten Leistung bzw. für eine nachträgliche Beauskunftung über diese nötig sind.

2.16 Datenverarbeitung

Die Korrespondenz mit dem Kunden oder einer Behörde gehört zu den im § 212 UGB erwähnten "Handelsbriefen", für die die dort normierte Aufbewahrungspflicht gilt. Weiters listet die Tabelle A.6 jene Datenkategorien auf, die dafür in Frage kommen.

2.17 Geldwäsche (SA037)

Die Berufsrechtnovelle BGBl I 135 / 2017 setzt im Wesentlichen im 2. Abschnitt (§§ 43 ff) die 4. EU-Geldwäsche-RL[26] zur Verhinderung der Geldwäsche und der Terrorismusfinanzierung um, indem einerseits das BiBuG novelliert wird und andererseits das WiEReG geschaffen wurde. Diese Novelle und das WiEReG sollten daher als Einheit gelesen werden.

Mit der BiBuG Novelle wird das bisherige starre Prüfschema durch einen risikobasierten Ansatz abgelöst. Dies bedeutet einerseits mehr Aufwand bei der Implementierung der nötigen Risikomanagement-Prozesse, andererseits darf erwartet werden, daß der risikobasierte Ansatz in der täglichen Praxis flexibler ist, als das alte starre Prüfungsschema.

Art. 33 der Richtlinie schreibt den Grundsatz "im Zweifel vernadern" vor, indem eine Meldepflicht statuiert wird, wenn der "Verdacht oder berechtigter Grund zu der Annahme" vorliegt oder "Kenntnis davon erhält", daß Gelder mit den zu bekämpfenden Vorgängen in Verbindung stehen.

Die von der Aufsichtsbehörde erlassene Bilanzbuchhaltungsberufe-Ausübungsrichtlinie 2017 (BB-AR 2017) ist anzuwenden. Bei Kunden, für die ausschließlich die Personalverrechnung durchgeführt wird, kann nur eine Warnung bei vermuteter mißbräuchlicher (Schein)Anmeldung von Dienstnehmern ausgesprochen werden.

Soweit nicht durch das BiBuG oder den BB-AR vorgegeben, kommt der vom Fachverband UBIT herausgegebene Kurzleitfaden[27] zur Anwendung.

2.17.1 Zweck der Datenverarbeitung

Mit diesen gesetzlichen Bestimmungen werden Maßnahmen zur Verhinderung der Geldwäsche und der Terrorismusfinanzierung im Berufsrecht ausgestaltet.

[26] RL 849 / 2015 / EU
[27] Siehe 5.

Risikobasierter Ansatz

Solange nur eine Person für die Kundenbuchhaltungen zuständig ist, kann der Aufbau der betriebsinternen risikobasierten Ausgestaltung der innerorganisatorischen Ausgestaltung entfallen.

In das kundenbezogene Risikomanagement kann nur das einbezogen werden, was der Kunde freiwillig offenlegt. Ein Pflicht zur Offenlegung besteht nur gegenüber den Abgabenbehörden. Eventuell meldepflichtige Anomalien können nur anhand der Buchungsfälle feststellbar sein[28]. In einer Gesamtschau der bekannten Umstände und der zu beurteilenden Geschäftsfälle, unter Berücksichtigung des üblichen Geschäftsverlaufes[29], kann sich die Meldepflicht[30] einzelner Geschäftsfälle ergeben.

Sorgfaltspflichten

Diese werden von den §§ 45 ff BiBuG bzw. den §§ 14 ff BB-AR 2017 vorgegeben. Eine darüberhinaus gehende Dokumentation der verwendeten Strategien, Kontrollen und Verfahren fällt unter Betriebs- und Geschäftsgeheimnis.

Der Grundsatz "Keine Buchung ohne Beleg", ermöglicht grundsätzlich eine 100% Prüfung aller offen gelegten Geschäftsfälle. Sollte sich daraus ein Verdachtsmoment ergeben, kommt eine zu erstattende Meldung in Frage.

Die Mitwirkung der BhB an Transaktionen beschränkt sich auf das Definieren der Zahlungen an die Abgabenbehörden im NetBanking des Kunden - unter der Voraussetzung, daß dies vom Kunden gewünscht wird. Die Prüfung und Freigabe dieser Zahlungen verbleibt beim Kunden.

Soweit nicht durch das BiBuG oder den BB-AR vorgegeben, kommen die vom Fachverband UBIT herausgegebenen Leifäden zur Annahme eines neuen Mandanten[31] bzw. der zur Verdachtsmeldung[32] zur Anwendung.

2.17.2 Dauer der Datenaufbewahrung

Die im § 52c umgesetzte fünfjährige Aufbewahrungspflicht[33], ab dem Ende der Geschäftsbeziehung, ist kürzer als die vom Abgabenrecht normierte siebenjährige Aufbewahrungsfrist bzw. die vom § 18 Abs. 10 UStG definierten 22 Jahre. Wird allerdings bekannt, daß ein gerichtliches Strafverfahren durchgeführt wird, endet die Aufbewahrungpflicht frühestens fünf Jahre nach Beendigung des Verfahrens. Zu beachten ist weiters die (maximal) fünfjährige Verjährungsfrist der §§ 31 f FinStrG. Zur Anwendung kommt das späteste anzuwendende Datum für das Ende der Aufbewahrungsfrist nach Berücksichtigung obiger anzuwendender Vorschriften. Die allgemeine Verjährungsfrist von 30 Jahren des § 1478 ABGB kann somit überschritten werden.

[28] "faktengestützte Entscheidungsfindung" im Erw.Gr. 22 der RL 849/2015/EU.
[29] Siehe § 19 BB-AR 2017.
[30] In einer ex ante Beurteilung.
[31] Siehe 3.
[32] Siehe 4.
[33] Art. 40 RL 849/2015/EU

2.17.3 Empfänger

Empfänger von Meldungen nach diesen Bestimmungen ist die im § 52a BiBuG definierte Geldwäschemeldestelle.

2.17.4 Datenverarbeitung

In Frage kommen alle Daten, Informationen und Dokumente, um die in den §§ 43 f BiBuG genannten Sorgfalts- und Prüfpflichten nachkommen zu können. Die zu verarbeitenden Datenkategorien werden im Gesetzestext des BiBuG aufgelistet.

2.18 WiEReG

Das Wirtschaftliche Eigentümer Registergesetz (WiEReG) ist Teil der nationalen Umsetzung der 4. EU-Geldwäsche-RL und normiert u.a. Rechte und Pflichten von Berufsberechtigten iSd BiBuG. Die Verweise beziehen sich auf das BGBl I 136 / 2017 idF BGBl I 62 / 2019, wobei Art. 1 des BGBl I 136 / 2017 jene EU-Richtlinien auflistet, die zur Vermeidung von Geldwäsche und Terrorismusfinazierung umgesetzt werden..

2.18.1 Zweck der Datenverarbeitung

Zweck dieser Bestimmungen ist es, den wirtschaftlichen Eigentümer gem. der Legaldefinition des § 2 WiEReG festzustellen und im Register gem. § 7 WiEReG einzutragen.

Rechte und Pflichten des Eigentümers

Da nicht jeder Rechtsträger automatisch auch der wirtschaftliche Eigentümer ist, haben sowohl der Rechtsträger (als juristische Person) als auch der wirtschaftliche Eigentümer (jene natürliche Person, die beherrschenden Einfluß auf die Tätigkeit des Rechtsträgers ausüben kann) Rechte und Pflichten iSd WiEReG.

Befreiung von der Meldepflicht

Die Buchhaltung Blaschka GmbH ist gem. § 6 Abs. 1 von der Meldepflicht befreit, da alle Gesellschafter natürliche Personen sind. Sollte es zu einer Änderung bei den Gesellschaftern kommen, wird eine Meldung nach § 5 Abs. 1 vorgenommen werden. Darüber hinaus kann die Richtigkeit der Daten in diesem Register jederzeit mittels Einsichtnahme in das Firmenbuch überprüft werden.

Die BhB GmbH als Verpflichteter

§ 9 Abs. 1 Z. 10 zählt die Berufsberechtigten gem. BiBuG zu den Verpflichteten, denen ebenfalls Rechte und Pflichten auferlegt sind.

Einsicht der Verpflichteten in das Register

Zu den Rechten gehört die Einsichtnahme in das Register der wirtschaftlichen Eigentümer - dazu wurden die Berufsrechte im BiBuG[34] entsprechend erweitert. Im Hinblick auf die BiBuG Novelle ist dies auch als Pflicht zu verstehen.

Sorgfaltspflichten der Verpflichteten gegenüber Kunden

§ 11 Abs. 1 verlangt u.a. als Sorgfaltspflicht gegenüber Kunden, daß nicht ausschließlich auf die im Register enthaltenen Daten vertraut werden darf. Die Verpflichteten haben nach einem risikobasierten Ansatz vorzugehen - dies deckt sich mit der berufsrechtlichen Anordnung des § 44 BiBuG.

Weiters normiert Abs. 3 eine Meldepflicht an das Register und Abs. 7 schließt deswegen eine Inanspruchnahme des Verpflichteten auf Schadenersatz aus. Dieser Ausschluß ergibt sich aus der Durchbrechung der Verschwiegenheitspflicht (§ 39 BiBuG) und der ausdrücklichen Anordnung im Art. 37 RL 849/2015/EU.

Die erläuternden Bemerkungen gehen davon aus, daß die Qualität der Daten im Register durch die, beim Verpflichteten zu implementierenden risikobasierten Prozesse, gesteigert werden kann und zu einer Entlastung der Nachforschungspflicht bei den Behörden führen wird. Womit der Verwaltungsaufwand und das Tragen des Risiko auf die Wirtschaftsteilnehmer abgewälzt wurde[35].

Die Praxis wird zeigen, ob die Erwartungen des Gesetzgebers auf Entlastung der Behörden in Erfüllung gehen werden.

Abgabenrechtliche Änderung

Durch die Verlagerung der Meldepflichten zu den Verpflichteten iSd WiEReG, wurde auch die Erhebungspflicht der Abgabenbehörde im § 115 Abs. 1 BAO entsprechend eingeschränkt und auf den Steuerpflichtigen überwälzt[36].

2.18.2 Strafbestimmungen

Diese sind im § 15 als reine Finanzordnungswidrigkeiten ausgestaltet, wobei Abs. 5 anordnet, daß diese niemals von einem Gericht zu ahnden sind. Dies ist notwendig, da die Strafen bis zu €200.000,- betragen und die gerichtliche Zuständigkeit im FinStrG bei €100.000,- beginnt - und somit dem ordentlichen Rechtsmittelverfahren entzogen wurden.

2.18.3 Dauer der Datenaufbewahrung

Das WiEReG selbst nennt keine Aufbewahrungsdauer. Dessen Untergrenze wird mit der Dauer der Eigenschaft als wirtschaftlicher Eigentümer anzunehmen sein.

[34] § 2 Abs. Z. 8 bzw. § 3 Abs. 2 Z. 5 BiBuG
[35] "im Zweifel vernadern"
[36] "erhöhte Mitwirkungspflicht des Abgabenpflichtigen"

Die Obergrenze ist durch die Anwendung der relevanten Aufbewahrungsvorschriften ab Entfall der Qualifikation als wirtschaftlicher Eigentümer anzunehmen. Hier kommen insbesonders die Bestimmungen des Abgabenrecht, des Gesellschaftsrechtes bzw. des Firmenrechts zur Anwendung. Das Ende der Vertragsbeziehungen löst den Fristenlauf für die mögliche Löschung der Daten aus - siehe [§ 5 2].

2.18.4 Empfänger

Empfänger ist das nach § 7 WiEReG einzurichtende Register der wirtschaftlichen Eigentümer sowie die Geldwäschemeldestelle (§ 11 Abs. 3 WiEReG).

2.18.5 Datenverarbeitung

In Frage kommen alle Daten, Informationen und Dokumente, um als Verpflichteter, iSd § 9 Abs. 1 Z. 10 WiEReG, die im § 11 WiEReG normierten Sorgfaltspflichten zur Feststellung des wirtschaftlichen Eigentümers, der nach § 4 WiEReG zur Offenlegung verpflichtet ist, einhalten zu können. Die zu verarbeitenden Datenkategorien werden im Gesetzestext aufgelistet.

2.19 Art. 32

Die "Sicherheit der Verarbeitung" soll durch ein Bündel an Maßnahmen erreicht werden. Dazu gehören u.a. die Verwendung einer privaten Netzwerkadresse[37], ein Backup-Konzept (Abs. 1 lit. c) und organisatorische Maßnahmen (Abs. 4). Zu den organisatorischen Maßnahmen gehört u.a. die Verpflichtungserklärung der Dienstnehmer[38], und speziell die Schaffung von Risikobewußtsein, um beispielsweise nicht jede Mail "blind" zu öffnen. Die Details zum Abs. 1 lit. b sind als Betriebs- und Geschäftsgeheimnis klassifiziert und an anderer Stelle dokumentiert.

Aus der Auswertung der anfallenden Daten ist bekannt, daß am SSH-Port in jeder Sekunde bis zu drei parallele Angriffe stattfinden. Beim Mail-Sub-System (Port 25) kommt es im Durchschnitt alle 15 Sekunden zu einem Versuch, die Sicherheitsmaßnahmen auszuhebeln. ftp (Port 21) wird mehrmals am Tag mit "Bulk Angriffen" konfrontiert. Der Web-Server liefert jeden Tag rd. 500 MB an Datenvolumen aus. Durch den konsequenten Einsatz von sicherheitsbewußten Open-Source-Produkten und der entsprechenden Konfiguration konnte noch kein gelungener Einbruchsversuch festgestellt werden.

2.19.1 Abs. 1 lit. c

Die verlangte Fähigkeit, bei einem physischen oder technischen Zwischenfall die Daten rasch wiederherstellen zu können, ist die Forderung ein Backup- bzw. Sicherungskonzept für die verarbeiteten Daten einzurichten und zu pflegen. Wobei diese Bestimmung mit dem Grundsatz der Speicherminimierung im Art. 5 (siehe Kapitel 2.2.5) konkurriert.

[37] iSd Internet Standard RFC 1918
[38] § 39 Abs. 5 BiBuG idgF

Die in Umsetzung der § 5 Abs. 5 und 6 [2] implementierten Konzepte sind als Betriebs- und Geschäftsgeheimnis klassifiziert und an anderer Stelle dokumentiert.

2.20 Art. 33

Die "Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde" kann nach einer Verletzung des Datenschutzes nötig werden. Im Einzelfall wird zu prüfen sein, welche Daten betroffen sind. Davon abgeleitet, kann eine Meldung an die Aufsichtsbehörde zu erstatten sein, wenn ein Risiko für die Rechte und Freiheiten natürlicher Personen festgestellt wird. Festzuhalten ist, daß nur solche Daten verarbeitet werden, für die es einen gesetzlichen Auftrag gibt.

2.21 Art. 34

Die "Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person" wird mit hoher Wahrscheinlichkeit nicht nötig werden, da diese Meldung ein **hohes** Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen als Voraussetzung hat.

Da die Datenverarbeitung auf gesetzlichen Vorgaben basiert, ist es auch nicht möglich, durch diese Datenverarbeitung in Rechte oder Freiheiten von natürlichen Personen einzugreifen, da dies bereits durch den Gesetzgeber erfolgt ist, der die Verarbeitung der Daten angeordnet hat.

Sollte eine Verletzung des Datenschutzes festgestellt werden, wird im Einzelfall zu prüfen sein, welche Daten betroffen sind. Davon abgeleitet kann eine Meldung an betroffene natürliche Personen zu erstatten sein.

2.22 Art. 35

Die "Datenschutz-Folgenabschätzung" ist durchzuführen, wenn die Datenverarbeitung **voraussichtlich** ein **hohes** Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Die Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutz-Folgenabschätzung[39] (DSFA-AV) nimmt alle in Anwendung befindlichen Datenverarbeitungen von der Durchführung einer Datenschutz-Folgenabschätzung aus.

2.23 Art. 37

Die "Benennung eines Datenschutzbeauftragten" ist nach Abs. 1 nicht nötig. Die BhB GmbH ist weder eine Behörde (lit. a), noch gehört es zur Kerntätigkeit, eine

[39] BGBl. II 108 / 2018

regelmäßige bzw. systematische Überwachung von betroffenen Personen durchzuführen (lit. b). Ebensowenig gehört die umfangreiche Verarbeitung besonderer Kategorien (iSv sensibler Daten) von Daten zur Kerntätigkeit (lit. c).

Auf das Recht, nach Abs. 2, freiwillig einen Datenschutzbeauftragten zu ernennen, wird verzichtet. Somit entfällt auch die Mitteilungspflicht nach Abs. 7.

2.24 Art. 40

Die BhB hat sich dem von der Datenschutzbehörde genehmigten Verhaltensregeln[40] unterworfen. Die Erstzertifizierung erfolgte am 11. März 2021. Die letzte Rezertifzierung erfolgte am 11. März 2024.

2.25 Art. 44

Die Übermittlung von personenbezogenen Daten in ein Drittland ist weder vorgesehen noch geplant. Jedoch kann nicht vollständig ausgeschlossen werden, daß dies beispielsweise bei einem Auftragsverarbeiter eines angeordneten Empfängers[41] der Fall ist. Die Sicherstellung des angemessenen Schutzniveaus ist in diesen Fällen in der Verantwortung des Empfängers.

2.26 Art. 88

Zu den Besonderheiten der Datenverarbeitung im Beschäftigungskontext sei auf Kap. 2.13 verwiesen.

[40] Siehe 2.
[41] Siehe Tabelle A.3.

Anhang A

Tabellen

Tabelle A.1: "Standard" Datenverarbeitungen

Code	Bezeichnung
SA001	Rechnungswesen
SA002	Personalverwaltung für privatrechtliche Dienstverhältnisse
SA022	Kundenbetreuung und Büroautomation
SA037	Melde- und Kontrollsystem zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung

Tabelle A.2: Kategorien betroffener Personen

Nr.	mögliche betroffene Person
01	der Kunde selbst, oder dessen (gesetzliche) Vertretung
02	Geschäftspartner des Kunden
03	Dienstnehmer des Kunden
04	Angehörige eines Dienstnehmers
05	Arzt, der z.B. eine Krankschreibung ausstellt
06	Gläubiger einer Exekution
07	Rechtsanwalt, der z.B. eine Lohnexekution betreibt
08	Gerichtsvollzieher, der (z.B.) eine Exekution ausführt
09	Masseverwalter
10	Gerichtskomissär eines Nachlasses

Tabelle A.3: mögliche Empfänger

Nr.	möglicher Empfänger
01	der Kunde selbst, oder dessen (gesetzliche) Vertretung
02	allgemein eine Behörde, an die eine Eingabe zu richten ist bzw. an die eine Meldung zu erstatten ist
03	die zuständige Landesstelle der ÖGK
04	Sozialversicherungsanstalt der Selbstständigen (SVS)
05	Bauarbeiter-, Urlaubs- und Abfertigungskassa (BUAK)
06	das zuständige Finanzamt (FA Österreich)
07	PLAB- bzw. Betriebsprüfer
08	Kommunalsteuer bzw. DGA Empfänger
09	Banken (z.B. für deren gesetzlich vorgeschriebene Risikobewertung)
10	Gerichte oder von diesen Bestellte
11	Inkassanten (im Fall von gerichtlich betriebenen Exekutionen)
12	Versicherungen (z.B. für die Prämienregulierung)
13	Statistik Österreich, für die gesetzlich angeordneten Meldungen
14	gesetzlich vorgebene Meldestelle
15	AUVA (z.B. für die Vergütung der Entgeltfortzahlung)

Tabelle A.4: Rechnungswesen

Nr.	Datenkategorie	Betr.	Empf.
01	Kunden-Id	01	-
02	Kundendaten, soweit diese für die Verarbeitung benötigt werden	01	02
03	Daten einer Gesellschaft, soweit diese benötigt werden	02	02
04	Daten eines Gesellschafters, soweit diese benötigt werden		02
05	Daten von dessen Kunden, im Falle der Doppik	02	07
06	Daten von dessen Lieferaten, im Falle der Doppik	02	07
07	für den Buchungsfall relevante Daten	02	07
08	zu verbuchende Kontoauszüge		07
09	zu verbuchende Kassabelege		07
10	zu verbuchende Eingangsrechnungen	02	07
11	zu verbuchende Ausgangsrechnungen	02	07
12	zu verbuchende Belege von einer Behörde	01	07
13	zu meldende Ergebnisse	01	06, 09, 12 - 14

Tabelle A.5: Personalverrechnung

Nr.	Datenkategorie	Betr.	Empf.
01	Kunden-Id	01	-
02	Personalnummer	03	-
03	Mitarbeiterdaten, soweit diese benötigt werden	03	03, 05, 07
04	Einstufung im Kollektivvertrag	03	07
05	Beitragsgrundlagenmeldung (mBGM)	03	03
06	BUAK Meldedaten und Meldungen	03	05
07	An-, Ab- und Änderungsmeldungen	03	03, 05
08	EFZ Vergütungsantrag	03	15
09	Arbeits- und Entgeld Meldung Krankenstand (AEK)	03	03
10	Arbeits- und Entgeld Meldung Wochengeld (AEW)	03	03
11	Dienstverhinderungen (z.B. Krankenstand, Mutterschutz, ...)	03, 04, 05	03
12	laufende Abrechnung, inkl. Sonderzahlungen (UZ bzw. WR)	03	03, 07
13	Führen des Lohnkontos	03, 04	07
14	Verwalten von Sachbezügen, Prämien u.dgl.	03	07
15	Jahresmeldungen (z.B. L1, KommSt1, DGA)	03, 06	
16	Drittschuldnererklärungen (EDritt1, EDritt3)	03, 06, 07	11

Tabelle A.6: Büroautomation

Nr.	Datenkategorie	Empf.
01	Kunden-Id	-
02	TimeStamp eines Ereignisses	-
03	Anzahl / Menge bez. eines Ereignisses	-
04	Dauer / Länge bez. eines Ereignisses	-
05	Kundendaten, soweit diese für die Durchführung benötigt werden	-
06	Kundenwünsche bez. der Durchführung von Aufträgen	-
07	Notizen zur Geschäftsbeziehung	-
08	erhaltene Briefe	-
09	versandte Briefe	01, 02
10	erhaltene SMS	-
11	versandte SMS	01, 02
12	geführte Telephonate	-
13	erstattete ELDA Meldung	03
14	erhaltene ELDA Krankenstandsbestätigungen	-
15	FOnline Meldungen gem. Bevollmächtigung	06
16	durchgeführter PV Lauf	01, 02
17	vom e-BUAK Portal erhaltene Meldungen	-
18	via e-BUAK Portal zu erstattende Meldungen	05
19	Ergebnisse der durchgeführten Buchhaltung	01, 02
20	Daten, die zur Leistungabrechnung benötigt werden	-

Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik. *SiSyPHuS Win10. Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10*. URL: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Studien/SiSyPHuS_Win10/SiSyPHuS_node.html (besucht am 20. 03. 2021).

[2] Fachverband UBIT der Wirtschaftskammer Österreich. *Code of Conduct gem. Art. 40 DSGVO*. 23. Aug. 2019. URL: https://www.buchhaltung-blaschka.at/Doc/20201104_CoC.pdf.

[3] FV UBIT. *Checkliste zur Annahme eines neuen Mandanten*. URL: https://www.buchhaltung-blaschka.at/Doc/GW_CL_NK.pdf.

[4] FV UBIT. *Checkliste zur Verdachtsmeldung*. URL: https://www.buchhaltung-blaschka.at/Doc/GW_CL_VM.pdf.

[5] FV UBIT. *Leitfaden zur Verhinderung der Geldwäsche und Terrorismusfinanzierung*. URL: https://www.buchhaltung-blaschka.at/Doc/GW_LF.pdf.

[6] *ISO/TR 10013:2001. Guidelines for quality management system documentation*. 15. Juli 2001.

[7] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. *Datenschutz bei Windows 10. Prüfschema*. Version 1.0. URL: https://tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/beschluss_zu_top_13_win10_prufschema.pdf (besucht am 20. 03. 2021).

[8] *KRACK Angriff auf WPA2 (1)*. URL: https://www.heise.de/security/meldung/Details-zur-KRACK-Attacke-WPA2-ist-angeschlagen-aber-nicht-gaenzlich-geknackt-3862571.html (besucht am 17. 10. 2017).

[9] *KRACK Angriff auf WPA2 (2)*. URL: https://www.heise.de/security/artikel/KRACK-so-funktioniert-der-Angriff-auf-WPA2-3865019.html (besucht am 20. 10. 2017).

[10] *KRACK-Attacke*. URL: https://www.heise.de/newsticker/meldung/Linus-Torvalds-Will-Intel-Scheisse-fuer-immer-und-ewig-verkaufen-3934829.html (besucht am 17. 10. 2017).

[11] *RFC 1918. Address Allocation for Private Internets*. Feb. 1996.

Versionshistorie

Ver.	Gültig ab	Änderung(en)
2.3	2024-04-27	Kap. 1.1 iSd [Kap. 4.5.2.2 f in 6] ergänzt. Verweise innerhalb dieses Dokumentes ergänzt. Die CoC Zertifizierungen verlinkt.
2.2	2024-04-22	Kap. 2.6 erweitert.
2.1	2024-03-30	Diverse Überarbeitungen und die Ergebnisse der CoC Rezertifizierung eingearbeitet. Die ”ehemaligen” Art. 13, DVR und EuGW Dokus hier integriert.
2.0	2023-01-17	Rechtsformwechsel.
1.6	2021-03-20	Ergebnisse des CoC Audit eingearbeitet.
1.5	2021-02-21	Kapitel 2.2.5 modifiziert.
1.4	2021-02-18	Kapitel 2.20 modifiziert.
1.3	2021-01-23	Kapitel 2.5 und 2.6 modifiziert.
1.2	2019-08-24	DSB Urteil DSB-D123.589/0002-DSB/2019 vom 9. April 2019 eingearbeitet.
1.1	2019-06-28	Löschkonzept im Kap. 2.2.5 ergänzt.
1.0	2019-04-06	Initialversion durch Abspaltung.