Allianz Selbständiger Reiseunternehmen – Bundesverband e.V.

Zum Umgang mit diesem Text

Dies ist eine Text**vorlage** für ein Datenschutzkonzept für touristische Unternehmen.

Als Text**vorlage** muss der Text zwingend an die jeweiligen betrieblichen Gegebenheiten angepasst bzw. erweitert (Liste der Auftragsdatenverarbeitungsverträge!) werden.

Der Text liefert die **Vorlage** für ein grundlegendes Datenschutzkonzept (Abschnitt I), die Regelungen für die Technischen und organisatorischen Maßnahmen (TOM) (Abschnitt II), eine Verpflichtungserklärung zur Vertraulichkeit und Verschwiegenheit (Abschnitt III), ein Verfahrensverzeichnis (Abschnitt IV) und eine Liste der Auftragsdatenverarbeitungsverträge (Abschnitt V).

Damit sollten die wichtigsten und zentralen Punkte einer kleinen betrieblichen Datenschutzorganisation für ein durchschnittliches Reisebüro mit weniger als 10 Personen, die regelmäßig mit der Verarbeitung personenbezogener Daten beschäftigt sind, erfüllt sein. Der Text ist aber im Sinne der DSGVO und des BDSG nicht vollständig oder abschließend. Jedes Unternehmen muss selbst prüfen, welche weiteren Maßnahmen aufgrund der jeweiligen betrieblichen Gegebenheiten zur treffen sind!

Dieser Text ist als Vorlage zur Arbeitserleichterung gedacht. Er stellt keine Rechtsberatung dar und wird ohne jede Garantie auf Richtigkeit oder Wirksamkeit zur Verfügung gestellt.

Allianz Selbständiger Reiseunternehmen – Bundesverband e.V.

Datenschutzkonzept der [Firmenname]

Inhaltsverzeichnis


asr
Allianz Selbständiger
Reiseunternehmen –
Bundesverband e.V.

Allianz Selbständiger Reiseunternehmen – Bundesverband e.V.

Vorwort

Die Buchung und Abwicklung von Reisen ist immer schon dadurch gekennzeichnet, dass viele Informationen über die Reise selbst und auch über die Reisenden benötigt werden und diese elektronisch verarbeitet werden. Bei dieser Datenverarbeitung den Schutz personenbezogener Daten sicherzustellen, ist unser Ziel.

In diesem Konzept zum Datenschutz haben wir strenge Voraussetzungen für die Verarbeitung personenbezogener Daten von Kunden, Interessenten, Geschäftspartnern und Mitarbeitern geregelt. Diese entspricht den Anforderungen der Europäischen Datenschutzrichtlinie und stellt die Einhaltung der Prinzipien der in Deutschland und der EU geltenden nationalen und internationalen Datenschutzgesetze sicher.

Unsere Führungskräfte und Mitarbeiter sind verpflichtet, diese Richtlinie zum Datenschutz einzuhalten und die jeweiligen Datenschutzgesetze zu wahren.

I. Abschnitt: Datenschutz Konzept

1. Ziel der Datenschutzrichtlinie

Die [Firmenname] verpflichtet sich im Rahmen ihrer gesellschaftlichen Verantwortung zur Einhaltung von Datenschutzrechten auf der Basis von europaweit akzeptierten Grundprinzipien zum Datenschutz.

Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation der [Firmenname] als attraktiver Arbeitgeber. Die Datenschutzrichtlinie schafft eine der notwendigen Rahmenbedingungen für die Datenübermittlungen zwischen unseren Kunden, Partnern und Dienstleistern.

2. Geltungsbereich und Änderung der Datenschutzrichtlinie

Diese Datenschutzrichtlinie gilt für die [Firmenname] sowie ggf. verbundenen Unternehmen und deren Mitarbeiter. Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten. Personenbezogene Daten sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Bestimmbar ist eine Person z.B. dann, wenn der Personenbezug durch eine Kombination von Informationen mit auch nur zufällig vorhandenem Zusatzwissen hergestellt werden kann.

3. Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb die [Firmenname] unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt V.. Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden. Im Falle einer Datenübermittlung an einen Empfänger außerhalb die [Firmen-

name] in einem Drittstaat [Drittstaaten im Sinne der Datenschutzrichtlinie sind alle Staaten außerhalb der Europäischen Union/EWR. Ausgenommen sind Staaten, deren Datenschutzniveau von der EU Kommission als angemessen anerkannt worden ist.] muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt. Dies gilt ebenfalls nicht für die Weitergabe von personenbezogenen Daten in der Abwicklung eines Kunden-Auftrags (Buchung) an Leistungserbringer. Im Falle einer Datenübermittlung von Dritten an die [Firmenname] muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

4. Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.

1. Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Falls im Arbeitsverhältnis nach dem Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z.B. Personalakte) vorgesehen sind, so bleiben diese unberührt.

2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.

3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.

4. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten dann gesperrt werden.

5. Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehender schutzwürdiger Interessen müssen beachtet werden.

6. Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

5. Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen

Daten erhalten, wenn und soweit und in dem Umfang dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten. Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Vorgesetzte müssen ihre Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

6. Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren. Die technisch organisatorischen Maßnahmen (TOM`s) zum Schutz personenbezogener Daten sind Teil des unternehmensweiten Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

Allianz Selbständiger Reiseunternehmen – Bundesverband e.V.

II. Abschnitt: Regelungen zur Umsetzung des Datenschutzes

1. Einhaltung von Rechtsvorschriften

Bei der Benutzung der IT-Systeme und Applikationen in unserem Unternehmen sind von den Mitarbeitern die geltenden Rechtsvorschriften zu Datenschutz und Datensicherheit sowie die Unternehmensregelungen einzuhalten. Dies sind insbesondere die Datenschutzrichtlinie und die IT-Richtlinie sowie die Richtlinie zur Nutzung von Internet, E-Mail und Dateiablagen. Sollten Mitarbeiter unsicher sein, ob und inwieweit Rechtsvorschriften oder Unternehmensregelungen einzuhalten sind, haben sie sich an ihren Vorgesetzten zur Klärung zu wenden.

2. Schulung

Die [Firmenname] trägt Sorge dafür, dass die Mitarbeiter die erforderlichen Schulungen und Instruktionen/Anweisungen erhalten, die für den jeweiligen Umgang mit den IT-Systemen und/oder Applikationen erforderlich sind. Außerdem werden regelmäßig Schulungen zum Thema Datenschutz und Datensicherheit abgehalten.

3. Allgemeine Regelungen

Die Nutzung der IT-Systeme und Applikationen im Unternehmen ist ausschließlich zu dienstlichen Zwecken und in jeweils erlaubten Umfang zur Aufgabenerledigung zulässig. Abweichungen hiervon bedürfen der ausdrücklichen Erlaubnis des Arbeitgebers, die schriftlich erfolgen muss.

Die Installation von Software zu privaten Zwecken ist untersagt. Im Übrigen darf nur die Software auf IT-Systemen des Unternehmens installiert werden, die vom Arbeitgeber oder der IT-Abteilung freigegeben worden ist. Die Benutzung privater Hard-und Software zu dienstlichen Zwecken ohne Genehmigung des Arbeitgebers ist nicht zulässig. Dies schließt insbesondere auch die Weiterleitung von dienstlichen E-Mail oder E-Mail Anhängen an private Konten oder das Speichern von dienstlichen Dateien auf privaten Systemen ein.

4. Arbeitsplatz

Der Arbeitsplatz ist von den Mitarbeitern so zu gestalten, dass Besucher oder sonstige Dritte keinen Zugang zu personenbezogenen Daten bekommen können, ohne hierfür berechtigt zu sein. So sind Büros nach dem Verlassen grundsätzlich zu verschließen. Außentüren von Bürogebäuden, Etagen oder ggf. einzelnen Räumen in fremden Gebäuden dürfen nicht offen gehalten werden und müssen sorgsam verschlossen werden. Beim Verlassen des Arbeitsplatz-PCs muss der jeweilige Mitarbeiter den Arbeitsplatz so „abmelden“ oder „sperren“, so dass vor der erneuten Nutzung des IT-Systems und/oder der Applikation(en) eine Authentifizierung (Benutzername/Passwort) erforderlich wird.

Informationen in Papierform sind so abzulegen, dass Besucher oder sonstige Dritte keine Kenntnisnahme von den Daten erhalten können. Vertrauliche Informationen sind stets unter Verschluss zu halten.

Im Falle das der Mitarbeiter einen vom Unternehmen genehmigten Homeoffice-Arbeitsplatz nutzt, sind zu den im Unternehmen selbst zu beachtenden Vorgaben zusätzliche Vorgaben zu beachten:

- Das Arbeitsmaterial muss den Standards des Unternehmens entsprechen. Dies schließt insbesondere ein, dass nur IT Systeme des Unternehmens für dienstliche Aufgaben benutzt werden dürfen.

- Die Zugänge zum Unternehmen müssen gesichert sein und die Daten verschlüsselt übertragen werden. Dies bedeutet insbesondere, dass nur über die Verbindung via VPN gearbeitet werden darf.

- Der Homeoffice Mittarbeiter hat dafür Sorge zu tragen, dass Dritten keine Möglichkeit geboten wird an Daten zu gelangen. Dies schließt insbesondere ein, dass das Ausspähen von Daten bei der Nutzung dienstlicher Systeme durch Dritte verhindert werden muss.

5. Passwort-Gebrauch

Soweit technisch möglich, sind alle IT-Systeme und Applikationen erst nach hinreichender Authentifizierung des Nutzers nutzbar. Die Authentifizierung erfolgt in der Regel durch die Verwendung der Kombination Benutzername/Passwort. Die IT-Abteilung wird, soweit keine betrieblichen oder technischen Gründe entgegen sprechen, jedem einzelnen berechtigten Nutzer einen Benutzernamen und ein Initial-Passwort zuweisen.

Passwörter müssen eine Mindestlänge von 8 Zeichen haben. Das Passwort ist alphanumerisch (Buchstaben und Zahlen/Zeichen mit Sonderzeichen) zu gestalten.

Soweit technisch möglich, ist jeder Mitarbeiter verpflichtet, sein Initial-Passwort unverzüglich zu ändern.

Die Passwörter sind so zu wählen, dass sie durch Dritte nicht leicht zu erraten sind. Vor-und Familiennamen oder Geburtstage, sowie Namen von Angehörigen sind nicht zur Passwortwahl geeignet. Gleiches gilt für trivial angeordnete Zahlenkombinationen (z.B. 12345).

Passwörter sollten regelmäßig gewechselt werden. Die bereits genutzten Passwörter dürfen nicht noch einmal wieder verwendet werden.

Die geforderte Komplexität der Passwörter und ihre regelmäßige Änderung soll technisch durch die jeweiligen Systeme sichergestellt werden.

6. Schutz vor Schad-Inhalten

Zum Schutz vor Schad-Inhalten werden im Unternehmen Virenschutzprogramme eingesetzt. Insbesondere eingehende E-Mail-Kommunikation wird durch die eingesetzten Virenschutzprogramme überprüft. Dabei kann es auch zur Löschung von E-Mails und Dateianhängen kommen. Für den Fall, dass ein Mitarbeiter eine E-Mail mit einem unbekannten bzw. verdächtigen Dateianhang erhält, ist

dieser verpflichtet, sich unverzüglich an die IT-Abteilung zu wenden. Der unbekannte bzw. verdächtige Dateianhang darf erst nach Freigabe durch die IT-Abteilung geöffnet werden.

Da Anhänge an E-Mails das primäre Einfallstor für Schadcode in das Unternehmensnetz sind, ist im Umgang mit E-Mails von nicht sicher bekannten Absendern äußerste Vorsicht geboten. Im Zweifelsfall ist immer Rücksprache zu nehmen.

7. Schutz vor unverlangter Werbung („Spam“)

Zum Schutz vor unverlangter Werbung durch E-Mail werden im Unternehmen so genannte Spam-Filter eingesetzt. Der Einsatz des Spam-Filters erfolgt aus betrieblichen Gründen. Durch den Spam-Filter kann es dazu kommen, dass im Einzelfall E-Mails unterdrückt oder gelöscht werden. Die Mitarbeiter sollen Sorge dafür tragen, dass zum Beispiel beim erwünschten Erhalt von E-Mail-Newsletter die entsprechenden Absender-Adressen in ihr E-Mail-Adressbuch gespeichert werden, um fehlerhafte Klassifizierungen zu vermeiden.

8. Nutzung von E-Mail/Internet

Soweit nicht ausdrücklich eine Zustimmung des Unternehmens erfolgt ist, darf die Nutzung von E-Mail und Internet nur für dienstliche Zwecke erfolgen. Näheres regelt eine entsprechende Richtlinie, die von jedem Mitarbeiter zu unterzeichnen ist.

9. Verhalten bei Sicherheitsvorfällen

Sollte der Mitarbeiter merken, dass der Schutz oder die Sicherheit von Daten in irgendeiner Weise gefährdet sein könnte, hat dieser sich unverzüglich an die IT-Abteilung und seinen Vorgesetzten zu wenden. Dies gilt insbesondere dann, wenn die Gefährdung sich auf personenbezogene Daten bezieht.

10. Datenschutz

Der rechtskonformen und sicheren Verarbeitung der personenbezogenen Daten kommt eine außerordentlich hohe Bedeutung zu. Sollte ein Benutzer Zweifel an der Rechtmäßigkeit oder Korrektheit des Umgangs mit personenbezogenen Daten haben, so ist Er oder Sie verpflichtet, sich dazu an den betrieblichen Datenschutzbeauftragten der [Firmenname] zu wenden. Dessen Person und Kontaktdaten sind auf der Internetseite und im Intranet hinterlegt.

11. Weisungen

Die Mitarbeiter sind verpflichtet, den Weisungen der IT-Abteilung Folge zu leisten. Sofern Zweifel an der Richtigkeit oder der Sinnhaftigkeit von Weisungen der IT-Abteilung bestehen, kann der Leiter der IT-Abteilung oder die Geschäftsführung eingebunden werden.

Allianz Selbständiger Reiseunternehmen – Bundesverband e.V.

III. Abschnitt: Verpflichtung zur Vertraulichkeit und Weisungsgebundenheit

1. Verpflichtungserklärung

Erklärung zur Vertraulichkeit und Weisungsgebundenheit für Mitarbeiter und Beschäftigten der [Firmenname und Adresse]:

Bei der [Firmenname] legen wir besonderen Wert auf die Vertraulichkeit im Umgang mit schutzbedürftigen Informationen.

Dabei genießen personenbezogene Daten besonderen gesetzlichen Schutz.

Personenbezogene Daten sind nicht nur die Daten, die sich konkret einer bestimmten Person zuordnen lassen (wie z.B. Name, Kontaktdaten, Beruf, Aufgabe im Unternehmen etc.), sondern auch die Daten, bei denen die Person erst über zusätzliche Informationen bestimmbar gemacht werden kann.

Wir gehen in unseren Unternehmen im Zweifel davon aus, dass ein Personenbezug einer Information vorliegt. Für personenbezogene Daten gelten dann die jeweils einschlägigen gesetzlichen Vorschriften zum Datenschutz wie z.B. die Datenschutz-Grundverordnung der Europäischen Union (nachfolgend „DSGVO“) und das Bundesdatenschutzgesetz („BDSG“).

Nach der DSGVO dürfen personenbezogene Daten nur dann verarbeitet werden, wenn es hierzu eine Rechtsgrundlage gibt oder der Betroffene eingewilligt hat. Die Daten dürfen grundsätzlich nur zu den vorgesehenen Zwecken verwendet werden. Bei der Verarbeitung der Daten ist insbesondere zu gewährleisten, dass die Integrität, Verfügbarkeit und Vertraulichkeit der personenbezogenen Daten gewährleistet ist.

In unserem Unternehmen bestehen Vorgaben und Geschäftsprozesse für die Verarbeitung personenbezogener Daten.

Für Sie konkret bedeutet diese Verpflichtung zur Vertraulichkeit, dass Sie Daten nur im Rahmen unserer internen Vorgaben verwenden und diese gegenüber Dritten vertraulich behandeln.

Darüber hinaus sind aber auch Betriebs- und Geschäftsgeheimnisse in unseren Unternehmen schutzbedürftige Daten. Eine Offenlegung von Betriebs- und Geschäftsgeheimnissen soll grundsätzlich nur dann erfolgen, wenn der jeweilige Vertrags- oder Geschäftspartner zuvor auf die Vertraulichkeit verpflichtet worden ist.

Wenn Sie hierzu Fragen haben oder sich im Zweifel unsicher sind, welche Regelungen zu treffen bzw. einzuhalten sind, können Sie sich jederzeit an Ihre/n Vorgesetzte/n wenden.

Ein Verstoß gegen Ihre Vertraulichkeitspflichten kann als arbeitsvertragliche Pflichtverletzung geahndet werden.

Darüber hinaus stellt eine unzulässige Verarbeitung von personenbezogenen Daten in bestimmten Fällen auch eine Straftat oder Ordnungswidrigkeit nach den §§ 42, 43 BDSG (s. Auszug der Strafvorschriften) dar.

Allianz Selbständiger Reiseunternehmen – Bundesverband e.V.

Beachten Sie ferner auch, dass bei einer unzulässigen Verarbeitung von personenbezogenen Daten durch unser Unternehmen Geldbußen von bis zu 20 Mio. Euro möglich sind. Wir sollten daher gemeinsam darauf achten, dass die Verarbeitung personenbezogener Daten in unserem Unternehmen in zulässiger Art und Weise erfolgt.

Diese Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

Etwaige andere Vertraulichkeitsvereinbarungen zwischen Ihnen und dem Unternehmen bleiben unberührt. Diese Vertraulichkeitsverpflichtung ersetzt jedoch eine ggf. erfolgte Verpflichtung zum Datengeheimnis nach dem BDSG a.F. mit Wirkung zum 25.05.2018.

Name der/des Beschäftigten:

Hiermit verpflichte ich mich zur Einhaltung der vorgenannten Regelungen zur Vertraulichkeit.

_____ _____

Ort, Datum Unterschrift der/des Beschäftigten

2. Auszug der Strafvorschriften:

Auszug aus dem Bundesdatenschutzgesetz (BDSG) in der ab 25.5.2018 geltenden Fassung:

§ 42 BDSG (neu) Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

ohne hierzu berechtigt zu sein, verarbeitet oder

durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 43 BDSG Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder

2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

Allianz Selbständiger Reiseunternehmen – Bundesverband e.V.

IV. Abschnitt: Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO

Zwecke der Verarbeitung

Tätigkeitsgegenstand ist die Vermittlung von Reisen.

Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

Kundendaten, Reisenden-Daten, Mitarbeiterdaten sowie Daten von Lieferanten sowie anderer Geschäftspartner, sofern die Verarbeitung zur Erfüllung der unter b. genannten Zwecke erforderlich ist. Details sind in der Anlage beschrieben.

Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

Kundendaten, Reisenden-Daten, Mitarbeiterdaten sowie Daten von Lieferanten sowie anderer Geschäftspartner, sofern die Verarbeitung zur Erfüllung der unter b. genannten Zwecke erforderlich ist. Details sind in der Anlage beschrieben.

Kategorien von Empfängern, denen die Daten offengelegt worden sind bzw. werden (intern/extern) sowie Empfänger in Drittstaaten

Hierzu zählen: Veranstalter, Beförderungsträger und andere Leistungsträger sowie Empfänger von Einreiseinformationen zur Durchführung der Buchungsanfragen und Buchungen; in Drittstaaten gemäß Art. 49, li. b, c DSGVO. Interne Empfänger sind Buchhaltung und Verwaltung.

Übermittlung in Drittstaaten

Eine Übermittlung an andere Unternehmen mit Sitz außerhalb der EU finden nur zur Durchführung der Buchungsanfragen und Buchungen gemäß Art. 49, li. b, c DSGVO statt. [ggf. bei Buchungssystemen im Ausland anzupassen]

Regelfristen für die Löschung der Datenkategorien

Der Gesetzgeber hat vielfältige Aufbewahrungspflichten und -fristen erlassen. Nach Ablauf dieser Fristen werden die entsprechenden Daten routinemäßig gelöscht. Sofern Daten hiervon nicht berührt sind, werden sie gelöscht, wenn ihre spezifischen Verarbeitungszwecke wegfallen. Die konkreten Löschfristen werden bei den jeweiligen Verfahren in der Anlage beschrieben.

Anlage zum Abschnitt IV: Verzeichnis der Verarbeitungstätigkeiten

Tabelle siehe separate Datei „Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 DSGVO Reisebüro Vorlage asr“

Allianz Selbständiger Reiseunternehmen – Bundesverband e.V.

V. Abschnitt: Liste der Auftragsdatenverarbeitungs-Vertragsverhältnisse

Mit den in der Anlage gennannten Unternehmen bestehen Auftragsdatenverarbeitungsverhältnisse.

Anlage zum Abschnitt V: Liste der Auftragsdatenverarbeitungs-Vertragsverhältnisse

Tabelle siehe separate Datei „Verzeichnis der Auftragsdatenverarbeitungsverträge Vorlage asr“