STORKE

Storks made easy

Datenschutzinformationen

Dokument

Version 1.2
App Version 1.0.0
Stand 27.09.2022

Dieses Dokument ist auch verfügbar unter: https://www.th-ab.de/studium/vor-dem-studium/studiengaenge-von-a-z/hebammenkunde
Der Inhalt gilt für die Testphase der App STORKE an der Hochschule Aschaffenburg.

Verantwortliche Stellen und Kontakt

Verantwortlicher für die Verarbeitung Ihrer personenbezogenen Daten ist die Hochschule Aschaffenburg und die Entwickler. Diese Datenschutzinformationen gelten für die Datenverarbeitung durch:

Technische Hochschule Aschaffenburg
Würzburger Str. 45
63743 Aschaffenburg

Telefon: 06021 42060
Web: https://www.th-ab.de

Datenschutzbeauftragter der Hochschule: datenschutz@th-ab.de
Mail der Entwickler: storke@th-ab.de

Inhalt

1. Einführung

Durch die Nutzung des Services der App STORKE vertrauen Sie uns (Entwickler im Namen der Hochschule Aschaffenburg, kurz „Entwickler“, „wir“, „uns“) Ihre Daten an. Der Schutz dieser Daten ist für uns von höchster Priorität. In diesem Dokument stellen wir dar, welche Daten von uns verarbeitet werden, zu welchem Zweck wir diese Daten verarbeiten und welche Rechte Ihnen in Bezug auf Ihre Daten zustehen.
Seit dem 25. Mai 2018 gelten im Bereich Datenschutz europaweit die einheitlichen Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO). Für eine Nutzung unserer Services ist es erforderlich, dass Sie der in dieser Datenschutzerklärung beschriebenen Verarbeitung personenbezogener Daten zustimmen. Diese Datenschutzerklärung wird unter Umständen in regelmäßigen Abständen geändert. Nur so können wir gewährleisten, dass Sie bestmöglich über die Verarbeitung Ihrer Daten informiert sind und wir die gesetzlichen Vorgaben zum Datenschutz einhalten. Sollten vorgenommene Änderungen für Ihre Einwilligung und die zugrundeliegenden Angaben maßgeblich sein, werden wir Sie über diese Änderungen in Kenntnis setzen, bevor Sie unsere Dienste nutzen.

Die Entwickler haften nicht für zweckentfremdete und unachtsame Nutzung der App STORKE.

Bitte lesen Sie sich unsere Datenschutzinformationen aufmerksam durch. Bei weiteren Fragen können Sie uns gerne mittels der im oberen Bereich dieser Datenschutzerklärung aufgeführten Kontaktdaten kontaktieren.

2. Verarbeitungstätigkeiten und Art und Zweck der Datennutzung

Wir verarbeiten bei der Nutzung unserer Services personenbezogene Daten. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen Art. 4 Abs.1 DSGVO. Im folgenden Abschnitt beschreiben wir demgemäß die Verarbeitung Art. 4 Abs.2 DSGVO solcher Daten, die Ihnen oder Dritten zugeordnet werden können.

Weiterhin werden Unterschriften, Aufenthaltsorte und Gesundheitsdaten gespeichert.

2.1 Datenverarbeitung bei der Nutzung der App STORKE

2.1.1 Erstellung eines Nutzerkontos (In der Testphase)

- Kategorien Personenbezogener Daten: E-Mail-Adresse und Kennwort, Name und Vorname, Zahlungsdaten.
- Zweck der Verarbeitung: Die genannten Daten werden verwendet, um Ihnen ein Nutzerkonto und den Zugang zu diesem Nutzerkonto zur Verfügung zu stellen. So können wir Ihnen die in unserer App enthaltenen Services anbieten.
- Rechtsgrundlage der Verarbeitung: Die dargestellte Verarbeitung erfolgt auf Grundlage der Einwilligung zur Nutzung dieser App Art.6 Abs 1 lit a und b DSGVO.
- Speicherdauer: Ihre Daten werden so lange gespeichert, wie das Vertragsverhältnis besteht oder sie ihr Nutzerprofil löschen. Dann werden die Daten gelöscht oder unumkehrbar anonymisiert. Für Studierende werden die Daten nach ihrem Studium automatisch gelöscht.

2.1.2 Datenverarbeitung beim „Pairing des Accounts“ (Verbinden mit einem Professor/ einer Professorin) (in der Testphase)

In der Testphase werden die Accounts der Studierenden, vom Entwickler, zu den verantwortlichen Professoren zugeordnet. Dies geschieht durch eine Rollenverteilung, die in der Datenbank hinterlegt ist. Die daraus abgeleiteten Rechte und Regeln werden im Kapitel „5. Berechtigungen in Bezug zur Rollenverteilung“ beschrieben.

2.1.3 Datentransfer über automatische Mails und PDF- Export

Von der App STORKE generierte PDFs können Dokumente (Protokolle, Anwesenheiten und Nachweise) und personenbezogene Daten erhalten. Sowohl die Studierenden selbst als auch die Professoren können Daten der Studierenden exportieren.

Durch Unterschreiben von Dokumenten (Protokolle und Anwesenheiten) werden automatische E-Mails generiert, die nur an die vom Nutzer definierten E-Mail-Adressen geschickt werden. Der Nutzer muss sich darüber im Klaren sein, dass seine Dokumente und personenbezogene Daten an die Besitzer dieser E-Mail-Adresse weitergegeben werden. Die Entwickler haften nicht, bei Datentransfer über diesem Weg.

Wir weisen darauf hin, den Datentransfer mit Umsicht zu benutzen.

2.1.4 Speichern von Daten aus klinischen Einrichtungen

Zu den klinischen Einrichtungen zählen Krankenhäusern mit stationären und ambulanten Einrichtungen, sowie weitere Geburtsstätten von Hebammen. Die dort erlernten Tätigkeiten und durchgeführten Nachweise können durch Freitextfeldern in der App STORKE niedergeschrieben werden. Darunter fallen Einträge, wie Gesundheitsdaten und personenbezogene Daten von Kindern, die durch Studierende getätigt werden. Diese Daten gehören zur Datenkategorie der besonderen Daten Art. 9 DSGVO und müssen daher mit Achtsamkeit behandelt werden. Die Eingaben müssen vom Nutzer verfremdet, nicht namentlich oder nicht einer Person identifizierbar eingetragen werden. Grundlage ist § 203 des Strafgesetzbuchs über Verletzung von Privatgeheimnissen. Ein Nutzer und nicht die Entwickler machen sich bei Unachtsamkeit und Verletzung dieses Gesetzes strafbar.

2.1.5 Logfiles und Geräteinformationen

Bei jedem Zugriff auf die App STORKE werden Anmeldeinformationen und Eigenschaften Ihres jeweiligen Endgerätes an den Server unserer Applikation gesendet und temporär in Protokolldateien, den sogenannten Logfiles, gespeichert. Die dabei gespeicherten Datensätze enthalten die folgenden Daten, die bis zur automatischen Löschung gespeichert werden:

- Datum und Uhrzeit des Abrufs
- Datum und Uhrzeit des Anmeldung
- Geräte-Version und Marke
- Rolle des Kontos
- Studenten-ID (Nur für Studenten)
- ID des Benutzers

Rechtsgrundlage für die Verarbeitung ist Artikel 6 Absatz 1 Buchstabe f) DSGVO. Unser berechtigtes Interesse ergibt sich aus der Gewährleistung eines reibungslosen Verbindungsaufbaus, Gewährleistung einer komfortablen Nutzung unserer Applikation, Auswertung der Systemsicherheit und -stabilität.

Ein unmittelbarer Rückschluss auf Ihre Identität ist anhand der Informationen nicht möglich und wird durch uns auch nicht gezogen warden. Die Daten werden gespeichert und nach Erreichung der vorgenannten Zwecke automatisch gelöscht. Die Regelfristen zur Löschung richten sich nach dem Kriterium der Erforderlichkeit.

2.2 Einwilligung

2.2.1 Verarbeitung im Rahmen der Testphase

- Um eine dauerhaft die technische Funktionsfähigkeit unserer App, sowie auch zukünftig eine möglichst nutzerfreundliche Umgebung zu gewährleisten, werden die Daten für die Weiterentwicklung der App genutzt.
- Um die Weiterentwicklung im frühen Stadium zu garantieren, werden die Daten nicht anonymisiert. Die Entwickler können die Daten eindeutig einer E-Mail-Adresse und dem selbst eingegebenen Namen zuordnen.

3. Von der App angeforderte Berechtigungen und deren Verwendung

3.1 Mobile Daten

- Die Nutzung der App benötigt eine Internetverbindung. Genutzt wird W-Lan oder die mobile Datenverbindung des Gerätes

4. Verarbeitung von Daten Dritter

Insbesondere in Bezug auf das besondere Verhätnis zwischen Studierenden und Professoren einer Hochschule kommt es in Betracht, dass Sie unsere Services im Auftrag eines Dritten nutzen. Die in dieser Datenschutzerklärung enthaltenen Verweise auf „Ihre Daten“ schließen die uns von Ihnen über dritte Personen zur Verfügung gestellten Daten mit ein.

5. Berechtigungen in Bezug zu Rollenverteilungen

Es gilt, verschiedene Personengruppen zu unterscheiden, da sich für Personen unterschiedliche Berechtigungen ableiten. Aufgezählt werden sowohl aktive Nutzer (haben einen Account bei STORKE), als auch passive Nutzer (haben keinen Account bei STORKE) und Personen, deren Daten aufgenommen werden.

Die Entwickler haben Adminrechte und können zu Testzwecken und für Verbesserungen an der Anwendung die Daten lesen, bearbeiten, schreiben und löschen.

5.1 Professoren

Erklärung der Rolle (Interner Empfänger):
Professoren können sich die Inhalte ihrer Studierenden anzeigen lassen, indem sie zwischen den Konten der Studenten wechseln. Sie können die Einträge der Studenten in zusammengefasster Form als Dokument exportieren.

Berechtigungen:
- Lesen von Daten der Studierenden
- Lesen, schreiben und löschen von eigenen Daten

5.2 Studierende

Erklärung der Rolle:
Studierende dokumentieren Anwesenheitszeiten, Praxisanleitungsprotokolle, und Nachweise. Diese sind auf einem Server gespeichert und können mit einer Internetverbindung von überall abgerufen werden. Eine Monatsansicht listet die Anwesenheitszeiten in grafischer Form auf. Unterteilt in die Abteilungsbereiche (Krankenhaus, freiberufliche Hebamme, etc.) sind genaue Verteilungen von Fehlzeiten, Arbeitszeiten und Urlaubszeiten einzusehen, sodass schnell ersichtlich ist, ob eine Abteilung möglicherweise zu kurz besucht wurde. Die Einträge zur Anwesenheit und den Praxisanleitungsprotokollen können bearbeitet oder zur Gegenzeichnung von der Praxisanleitung freigegeben werden. Auf nahezu jedem Bildschirm sind Fortschrittsbalken zu finden, die den aktuellen Stand der Einträge wiedergeben.

Berechtigungen:
- Lesen, schreiben und löschen von eigenen Daten

5.3 Praxisanleitung

Erklärung der Rolle (Interner Empfänger):
Die **Praxisanleitung** unterzeichnet die Einträge der Studierenden auf deren Bildschirm. Über eine separate Seite in der STORKE-App können die Studierenden ihre zu unterschreibenden Dokumente organisieren. So lassen sich zum einen Anwesenheiten und Praxisanleitungsprotokolle zu Personen und Orten zuordnen. Zum anderen wird der Praxisanleitung eine praktische Zusammenfassung der zu unterschriebenen Inhalten geboten. Die unterschriebenen Dokumente können an eine E-Mail-Adresse der Praxisanleitung zugeschickt werden. Die Unterschrift wird gespeichert und kann auf die Dokumente gedruckt werden.

Berechtigungen (ohne eigenen Account):
- Lesen von ausgewählten Daten. Studierender gibt Inhalte vor.

5.4 Externe Empfänger

Erklärung der Rolle:
Zum Abschluss der Hebammenausbildung werden exportierte PDFs der Prüfungskommission vorgelegt.

Berechtigungen (ohne eigenen Account):
- Lesen von PDFs

6. Gewährleistung der Datensicherheit

Wir versichern eine bestmögliche Datensicherheit zu gewährleisten. Dabei sind uns die folgenden Aspekte besonders wichtig:
- Der Zugriff auf personenbezogene Daten wird intern auf den nur unbedingt notwendigen Personenkreis beschränkt.
- Die Daten sind verschlüsselt auf dem Server gespeichert.
- Wir arbeiten daran, die Verschlüsselung der Daten bei der Übertragung zu garantieren.
- Jeder Zeit gewähren wir Einblick in alle gespeicherten Daten.
- Der Zugang zur App wird durch eine Zwei-Faktor-Authentifizierung gesichert.

6.1 Datenbank

Wir verwenden in unserer APP Firebase, als Webhosting- und Cloud-Dienst. Dienstanbieter ist das amerikanische Unternehmen Google Inc. Für den europäischen Raum ist das Unternehmen Google Ireland Limited (Gordon House, Barrow Street Dublin 4, Irland) für alle Google-Dienste verantwortlich. Die von uns benutzen Server befinden sich nach Auskunft von Google in Frankfurt am Main.
Google kann durch die Standardvertragsklausel Daten von Ihnen u.a. auch aus der USA verwalten. Wir weisen darauf hin, dass nach Meinung des Europäischen Gerichtshofs derzeit kein angemessenes Schutzniveau für den Datentransfer in die USA besteht. Dies kann mit verschiedenen Risiken für die Rechtmäßigkeit und Sicherheit der Datenverarbeitung einhergehen.
Als Grundlage der Datenverarbeitung bei Empfängern mit Sitz in Drittstaaten (außerhalb der Europäischen Union, Island, Liechtenstein, Norwegen, also insbesondere in den USA) oder einer Datenweitergabe dorthin verwendet Google sogenannte Standardvertragsklauseln (= Art. 46. Abs. 2 und 3 DSGVO). Standardvertragsklauseln (Standard Contractual Clauses – SCC) sind von der EU-Kommission bereitgestellte Mustervorlagen und sollen sicherstellen, dass Ihre Daten auch dann den europäischen Datenschutzstandards entsprechen, wenn diese in Drittländer (wie beispielsweise in die USA) überliefert und dort gespeichert werden. Durch diese Klauseln verpflichtet sich Google, bei der Verarbeitung Ihrer relevanten Daten, das europäische Datenschutzniveau einzuhalten, selbst wenn die Daten in den USA gespeichert, verarbeitet und verwaltet werden. Diese Klauseln basieren auf einem Durchführungsbeschluss der EU-Kommission.

6.2 Technische und Organisatorische Maßnahmen

Die Entwickler gewährleisten im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die gesetzlich geforderten Sicherheitsmaßnahmen und wird sie auf Verlangen des Nutzers nachweisen. Folgende besonderen technischen und organisatorischen Maßnahmen werden bei der Verarbeitung eingehalten und können durch eigene Leistung oder von Google Firebase durchgeführt werden:

6.2.1 Vertraulichkeit

a) **Zutrittskontrolle** (beispielsweise für Gebäude und Räume; an Schränke und Schächte)
Mindestmaßnahmen, mit denen Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:
- Sichere Schließanlage
- Zutrittskontrollsystem
- Überwachungseinrichtung, evtl. Einrichtung von Sicherheitszonen

b) **Zugangskontrolle** (keine unbefugte Systembenutzung, beispielsweise unerlaubtes Hochfahren oder unbefugte Anmeldung in Systemen)
Mindestmaßnahmen mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert werden:
- Passwortmechanismus (sicheres Passwort und regelmäßiger Passwortwechsel)
- Automatisches Sperren, Abmelden bei längerem Nicht-Gebrauch
- Firewall
- Virenschutz

c) **Zugriffskontrolle** (Anwendungen ausführen, unerlaubte Tätigkeiten in DV-Systemen und Zugriffe auf Daten, Applikationen und Schnittstellen verhindern)
Mindestmaßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, gelesen, kopiert, verändert oder entfernt werden können.:
- Differenzierte Berechtigungen für die DV-Systeme (Profile, Rollen)
- Regelmäßige Updates
- Implementierte und wirksame Löschkonzepte
- Verwendung geeigneter Pseudonymisierungsverfahren (In Testphase ausgesetzt)

d) **Trennungskontrolle**
Mindestmaßnahmen, die gewährleisten, dass personenbezogene Daten, die zu unterschiedlichen Zwecken und für verschiedene Auftraggeber erhobene Daten wurden, getrennt verarbeitet werden.
- Logische Speicherung der Kundendaten nach Mandanten
- Test und Produktionsdaten müssen in getrennten Systemen verarbeitet werden

6.2.2 Integrität

a) **Weitergabekontrolle**
Mindestmaßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:
- Verschlüsselte Übertragung und Speicherung nach Stand der Technik

b) **Eingabekontrolle** (Nachvollziehbarkeit, Dokumentation)
Mindestmaßnahmen, die gewährleisten, dass nachträglich überprüft werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt werden können:
- Monitoring und Log-Management
- Berechtigungsregelungen

6.2.3 Verfügbarkeit

Mindestmaßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust, gegen technische Störungen durch das Versagen der Betriebs-/Anwendungssoftware, vor fahrlässigen/vorsätzlichen Handlungen, vor schadenstiftender Software geschützt sind:
- regelmäßige Sicherungskopien
- Schutzsoftware vor Schadprogrammen
- logische Trennung

6.2.4 Belastbarkeit

Mindestmaßnahmen, die sicherstellen, dass im Falle eines Ausfalls der DV-Systeme diese rasch wiederhergestellt werden können.

6.3 Empfänger außerhalb der EU

Mit Ausnahme der dargestellten Verarbeitungen geben wir Ihre Daten nicht an Empfaenger mit Sitz ausserhalb der Europäischen Union oder des Europäischen Wirtschaftsraumes weiter. Die genannten Verarbeitungen bewirken eine Datenübermittlung an die Server der durch uns beauftragten Anbieter von Tracking- bzw. Targetingtechnologien. Die Datenübermittlung erfolgt auf Grundlage sogenannter Standardvertragsklauseln der EU-Kommission.

6.4 Datensicherheit

Alle von Ihnen persönlich übermittelten Daten, einschließlich Ihrer Zahlungsdaten, werden mit dem allgemein üblichen und sicheren Standard SSL (Secure Socket Layer) übertragen. SSL ist ein sicherer und erprobter Standard, der z.B. auch beim Onlinebanking Verwendung findet. Sie erkennen eine sichere SSL-Verbindung unter anderem an dem angehängten s am http (also https://...) in der Adressleiste Ihres Browsers oder am Schloss-Symbol im unteren Bereich Ihres Browsers.

Wir bedienen uns im Übrigen geeigneter technischer und organisatorischer Sicherheitsmaßnahmen, um Ihre bei uns gespeicherten persönlichen Daten gegen Manipulation, teilweisen oder vollständigen Verlust und gegen unbefugten Zugriff Dritter zu schützen. Unsere Sicherheitsmaßnahmen werden entsprechend der technologischen Entwicklung fortlaufend verbessert.

7. Ihre Rechte

7.1 Überblick

Um Ihre personenbezogenen Daten wirksam zu schützen, gewährt Ihnen das Datenschutzrecht eine Reihe von Rechten, die Sie gegenüber der Hochschule Aschaffenburg geltend machen können. Neben dem Recht auf Widerruf Ihrer uns gegenüber erteilten Einwilligungen stehen Ihnen bei Vorliegen der jeweiligen gesetzlichen Voraussetzungen die folgenden weiteren Rechte zu:

- Auskunft über die Verarbeitung (Artikel 15 DSGVO)
- Berichtigung unrichtiger Daten (Artikel 16 DSGVO)
- Löschung nicht mehr benötigter Daten (Artikel 17 DSGVO)
- Einschränkung der Verarbeitung (Artikel 18 DSGVO)
- Datenübertragbarkeit (Artikel 20 DSGVO)
- Widerspruch gegen die Verarbeitung (Artikel 21 DSGVO)

7.2 Widerspruchsrecht

Unter den Voraussetzungen des Art. 21 Abs. 1 DSGVO kann der Datenverarbeitung aus Gründen, die sich aus der besonderen Situation der betroffenen Person ergeben, widersprochen werden. Dazu zählt, dass die vorgenannten Rechte gegenüber der Hochschule Aschaffenburg und/oder den Entwicklern geltend gemacht werden können. Für die Geltendmachung reicht eine einfache Mitteilung an die in in dieser Datenschutzerklärung unter „Verantwortliche Stellen und Kontakt“ genannten Kontaktdaten.

Das vorstehende allgemeine Widerspruchsrecht gilt für alle in dieser Datenschutz-Information beschriebenen Verarbeitungszwecke, die auf Grundlage von Artikel 6 Absatz 1 Buchstabe f) DSGVO verarbeitet werden. Anders als bei dem auf die Datenverarbeitung zu werblichen Zwecken gerichteten speziellen Widerspruchsrecht, sind wir nach der DSGVO zur Umsetzung eines solchen allgemeinen Widerspruchs nur verpflichtet, wenn Sie uns hierfür Gründe von übergeordneter Bedeutung nennen (z.B. eine mögliche Gefahr für Leben oder Gesundheit).

Neben den vorgenannten Rechten haben Sie ein Beschwerderecht bei einer Datenschutz-Aufsichtsbehörde (Art. 77 DSGVO). Dieses Recht gilt unabhängig eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs.

8. Wichtige Hinweise und Tipps zum Schutz Ihrer Daten

In der vernetzten Welt von heute sind unbefugte Zugriffsversuche auf personenbezogene Informationen eine Realität, der sich Privatpersonen und Unternehmen tagtäglich aufs Neue stellen müssen. Das ist ohne Frage eine große Herausforderung.

Da Datenschutz bei uns allerhöchste Priorität hat, investieren wir in die Sicherheit unserer Systeme und kontrollieren diese stetig. Da auch Sie einiges tun können, um sich gegen den unbefugten Zugang Dritter zu Ihren Informationen zu schützen, wollen wir Ihnen an dieser Stelle einige Hinweise zum sicheren Umgang mit Ihren Informationen geben.

a) Wie kann ich meine personenbezogenen Informationen schützen?

Grundsätzlich gilt: Schützen Sie Ihr Benutzerkonto und auch Ihr Mobil-Gerät mit einem sicheren Passwort, das nur Sie kennen! Achten Sie außerdem darauf, sich regelmäßig abzumelden und ein neues Passwort festzulegen.

Stellen Sie sicher, dass Sie Ihre Passwörter immer nur für einen Account nutzen! Verwenden Sie nie ein Passwort für verschiedene Anbieter oder Portale.

Notieren Sie sich die Passwörter nicht an einem frei zugängigen Ort. Stellen Sie auch hier sicher, dass nur Sie Zugang zu den Passwörtern haben.

b) Wie erstelle ich ein sicheres Passwort?

Passwörter sollten so gewählt werden, dass sie nicht leicht erraten werden können, also z.B. keine gängigen Wörter aus dem Alltag, den eigenen Namen oder Namen von Verwandten. Um das Passwort noch sicherer zu machen, empfiehlt sich die kombinierte Verwendung von Groß- und Kleinschreibung, Zahlen und Sonderzeichen. Am bewährtesten ist ein gut merkbarer Spruch, der für ein Passwort verwendet wird. Die Auslegung unserer App enthält Regeln für ein starkes Passwort.

c) Gibt es weitere Dinge, die ich beachten sollte?

Sollten Sie ohne konkreten Kontakt unangeforderte E-Mails bekommen, in denen Sie gebeten werden, STORKE-Passwörter zu nennen oder Angaben zu Zahlungsdaten abzugeben, ignorieren Sie dies und nehmen Sie bitte unverzüglich Kontakt mit uns auf. Wir werden diese Vorfälle untersuchen.