



Datenschutz FAQs | Papershift

Gibt es bei Papershift einen Datenschutzbeauftragten?

Kann mit Papershift ein Auftragsverarbeitungsvertrag (AVV) geschlossen werden?

Wo werden die Daten in Papershift gespeichert?

Ist es möglich die personenbezogenen Daten unseres Account zu pseudonymisieren?

Wurde sichergestellt, dass die Unter-Auftragsverarbeiter von Papershift mit der aktuellen Rechtslage vertraut sind und sich entsprechend verhalten?

Ist es möglich, unseren Account auf eine konzentrierte Verarbeitung innerhalb der EU umzuschalten?

Wie geht Papershift mit dem ungültigen EU-US Privacy Shield um?

Erfolgt eine Übermittlung von Daten außerhalb des EWR-Raumes und wenn ja, auf welcher Grundlage erfolgt diese?

Gibt es Funktionseinschränkungen durch die Umschaltung auf die "EU"-Variante?

Gibt es eine ISO 27001 Zertifizierung?

Gibt es bei Papershift einen Datenschutzbeauftragten?

Papershift setzt in der Beratung von Datenschutzfragen auf die Verimax GmbH:

Verimax GmbH

Warndtstraße 115, 66127 Saarbrücken

Bei allen Fragen rund um das Thema Datenschutz wende dich bitte an **datenschutz@papershift.com**.

Kann mit Papershift ein Auftragsverarbeitungsvertrag (AVV) geschlossen werden?

Ja, wir bieten über unsere Website einen AVV an, der in elektronischer Form geschlossen werden kann. Die aktuelle Version findet sich unter

<https://www.papershift.com/datenschutz>

Wo werden die Daten in Papershift gespeichert?

Beim Hosting unserer Software setzen wir bei Papershift auf die Amazon Web Services (AWS), Serverstandort Frankfurt. Weitere Details zu den Datenschutz-

Maßnahmen von AWS gemäß DSGVO findest du hier:
<https://aws.amazon.com/de/compliance/gdpr-center/>

Ist es möglich die personenbezogenen Daten unseres Account zu pseudonymisieren?

Ja. Papershift und die darin enthaltenen Funktionen sind nicht von personenbezogenen Daten abhängig. Damit hast du bei uns die Möglichkeit mithilfe ganz einfacher Maßnahmen deinen Account und die personenbezogenen Daten von dir und allen Mitarbeitern zu pseudonymisieren. Wie kannst du das umsetzen? Einerseits ist es nicht erforderlich, Klarnamen zu verwenden. Du kannst statt Klarnamen Kürzel, Nummern oder andere Kodierungen verwenden, zu denen nur du die Entschlüsselung hast. Dadurch werden keine personenbezogenen Daten in Papershift angelegt und niemand hat Zugriff auf diese. Wenn du und die Nutzer deines Accounts IP-Blocker (z.B. VPN, Proxyserver, ...) nutzen, wird auch die personenbezogene IP-Adresse nicht mitgesendet. So kannst du unser Produkt nutzen ohne jegliche personenbezogenen Daten verwenden zu müssen. Auch ohne diese Maßnahmen kannst du dir sicher sein, dass wir bei Papershift bereits einen hohen Datenschutzstandard einhalten.

Wurde sichergestellt, dass die Unter-Auftragsverarbeiter von Papershift mit der aktuellen Rechtslage vertraut sind und sich entsprechend verhalten?

Mit allen Sub-Unternehmern wurden Auftragsverarbeitungsvereinbarungen oder sogenannte SCCs (Standard Contractual Clauses der EU) abgeschlossen. Bis zum EuGH-Urteil vom 16.07.2020 gab es auch Dienstleister in den USA die basierend auf dem EU-US-Privacy Shield mit uns kooperiert haben. Diese Verträge werden nun auf SCC umgestellt. Somit erfolgen zukünftig alle Datenübertragungen in Drittländer auf Basis der SCC.

Zusätzlich achten wir darauf, dass die TOM (technische und organisatorische Maßnahmen) unserer Sub-Unternehmen auf dem hohen, von uns geforderten, Standard liegen.

Ist es möglich, unseren Account auf eine konzentrierte Verarbeitung innerhalb der EU umzuschalten?

Du als Kunde hast bei uns die Möglichkeit, den Zugang mittels eines feingranularen Berechtigungskonzeptes selbst festzulegen. Wir bieten Dir mit der **"EU"-Variante** eine Lösung an, die die Verarbeitung Deiner Daten auf Sub-Unternehmern innerhalb

des EU-Raumes konzentriert. Der von uns ausgewählte Speicherort Deiner Daten liegt innerhalb der EU. Um die von Dir beauftragte Leistung jedoch vollumfänglich erbringen zu können, greifen in Einzelfällen Dienstleister aus Drittländern im Rahmen der Verarbeitungstätigkeiten auf diese Daten zu. Wir vereinbaren hierzu mit unseren Dienstleistern Datenschutzverträge basierend auf EU-Standardvertragsklauseln.

Wenn Du die Umstellung auf die **"EU"-Variante** vornehmen möchtest, kontaktiere bitte unser Service-Team unter support@papershift.com. Diese nehmen die Einstellung vor und bestätigen sie Dir.

Wie geht Papershift mit dem ungültigen EU-US Privacy Shield um?

Bei unserer Standard-Vertragsvariante kommen Sub-Unternehmen aus Drittländern wie bspw. den USA zum Einsatz, da wir hierdurch Ihnen, unseren Kunden, eine noch bessere und umfangreichere Beratungs- und Servicequalität bieten können.

Wie du sicherlich der medialen Berichterstattung entnommen hast, hat der EuGH in der Rechtssache C-311/18 zur Frage der Übermittlung von personenbezogenen Daten in Drittländer am 16.07.2020 eine weitreichende Entscheidung getroffen.

In dem Urteil geht es um die Rahmenbedingungen mit denen eine Übermittlung personenbezogener Daten an ein Unternehmen mit Firmensitz in den USA zulässig ist. Häufig wurde in der Vergangenheit mit amerikanischen Unternehmen basierend auf den bis zu dem Urteil gültigen Zertifikat (EU-US Privacy Shield) kooperiert. Gerne wurde dieses Zertifikat von amerikanischen Unternehmen erworben, um so ein angemessenes europäisches Datenschutzniveau ausweisen zu können.

Gegenstand des EuGH-Urteils ist nun, dass die Übermittlung personenbezogener Daten auf Basis des EU-US Privacy Shields gänzlich als unzulässig eingestuft wird. Die Verwendung von Standardvertragsklauseln oder Binding Corporate Rules (BCR) wird noch als Möglichkeit eines DSGVO-konformen Datenaustausches angesehen, allerdings muss hierfür sichergestellt sein, dass ein angemessenes europäisches Datenschutzniveau vorliegt. Im Rahmen unserer Kooperation mit Partnerunternehmen stellen wir an alle nationalen wie internationalen Partner gleich hohe Sicherheitsanforderungen, um einen einheitlichen Standard zu gewährleisten.

Als beauftragter Dienstleister können wir mit personenbezogenen Daten unserer Auftraggeber in Berührung kommen. Deshalb ist es stets unser Anliegen größtmögliche Datensicherheit in Verbindung mit sehr guter Performance und einfacher, kundenfreundlicher und intuitiver Bedienbarkeit in Einklang zu bringen.

Wir wählen unsere Kooperationspartner mit Bedacht aus und schließen mit ihnen entsprechende datenschutzrechtliche Verträge ab, um eine sichere Verarbeitung der Daten zu gewährleisten. Eine gänzliche Vermeidung eines transatlantischen Datenverkehrs läßt sich ist nach unserer Auffassung derzeit nicht realisieren. Dies

würde beispielsweise den E-Mail Verkehr beinhalten. Der Weg einer Mail kann nicht geplant werden, bzw. es kann nicht gänzlich ausgeschlossen werden, dass der Weg über einen Knotenpunkt in einem unsicheren Drittland (wie beispielsweise USA) erfolgt. Wenn man dies noch dezidierter betrachtet, so ist im Grunde der Einsatz eines US-amerikanischen Software- oder Hardware-Unternehmens prinzipiell risikobehaftet, da ein Zugriff US-amerikanischer Behörden denkbar erscheint. Dies würde aber dazu führen, dass innerhalb der EU, im Grunde bei deutlich mehr als 90% der Unternehmen die IT abgestellt werden müsste, da in der Regel immer in irgendeiner Form ein US-amerikanisches Produkt, sei es Hardware oder Software, zum Einsatz kommt.

Ob und inwieweit US-amerikanische Unternehmen den hier abgefragten Gesetzen unterliegen und zur Datenherausgabe im Einzelfall herangezogen werden, können wir als europäisches Unternehmen mit Sitz in Karlsruhe nicht beurteilen. Allerdings ist nach unserer Auffassung, die Wahrscheinlichkeit eines tatsächlichen Datenzugriffs durch die US-amerikanischen Ermittlungsbehörden, auf Daten die wir als Ihr Auftragsverarbeiter verarbeiten, als äußerst gering einzustufen. Die von uns verarbeiteten personenbezogenen Daten werden vermutlich von den US-amerikanischen Ermittlungsbehörden nicht als signifikante und somit erhebungsrelevante Daten eingestuft.

Wir bieten mit der „**EU**“ Variante eine Lösung an, die die Verarbeitung der personenbezogenen Daten auf Sub-Unternehmern innerhalb des EU-Raumes konzentriert.

Wir als Papershift-Team machen uns für stark für ein sicheres und performantes Produkt, bei dem die Datenspeicherung innerhalb der EU liegt. Wir werden weiterhin täglich hart daran arbeiten unser Produkt noch besser zu machen und betrachten dabei die Themen Datenschutz und Datensicherheit als essenzielle Bausteine unserer Unternehmensstrategie.

Erfolgt eine Übermittlung von Daten außerhalb des EWR-Raumes und wenn ja, auf welcher Grundlage erfolgt diese?

Datenübertragungen in Drittländer im Rahmen unserer Standard-Vertragsvariante erfolgen auf Basis der SCC (Standard Contractual Clauses / Standardvertragsklauseln der europäischen Union). Bis zum EuGH-Urteil vom 16.07.2020 gab es auch Dienstleister in den USA die basierend auf dem EU-US-Privacy Shield mit uns kooperiert haben. Diese Verträge werden nun auf SCC umgestellt.

Gibt es Funktionseinschränkungen durch die Umschaltung auf die "EU"-Variante?

Es gibt nur geringfügige Einschränkungen:

- Eingeschränkter Support

Gibt es eine ISO 27001 Zertifizierung?

Papershift selbst ist nicht nach der ISO 27001 zertifiziert. Aber AWS als einer unserer Sub-Unternehmer ist zertifiziert. Unter dem nachfolgenden Link kannst Du das Zertifikat aufrufen: <https://aws.amazon.com/de/compliance/iso-27001-faqs/>

Um eine sichere Datenverarbeitung zu gewährleisten führen wir regelmäßige Pentests durch und überprüfen unsere Systeme, mittels externer Untersuchungen, auf Schwachstellen:

https://cdn.papershift.com/20191202085049/00_AV-Anhang_Beschreibung_der_technischen_und_organisatorischen_Maßnahmen_TOM_02-12-2019.pdf