



# LastPass für Anwaltskanzleien

Anwaltskanzleien übernehmen Mandate von Unternehmen, Privatpersonen oder öffentlichen Institutionen. Sie beraten in rechtlichen Belangen, vertreten ihre Mandanten vor Gericht, verfassen Schriftsätze und kümmern sich um finanzielle Transaktionen.

## Mangelnde Sicherheit? Diese Akte kann jetzt geschlossen werden.

Anwaltskanzleien verwalten und verwahren im Rahmen ihrer Mandate hochsensible Daten und Dokumente – Finanzdokumente, Patentunterlagen, Gutachten, Verträge und mehr. Für Cyberkriminelle sind sie deshalb ein attraktives Angriffsziel. Der Diebstahl oder die Kompromittierung von Zugangsdaten können zu Datenschutzverletzungen, Betrug und Imageschäden führen. Gelangen vertrauliche Informationen in falsche Hände, werden Mandate entzogen und es drohen rechtliche und finanzielle Konsequenzen.

Eine weitere Herausforderung neben den Sicherheitsrisiken ist die Zugriffsverwaltung und Zusammenarbeit in der Kanzlei. Anwälte, ihr Assistenzpersonal und externe Geschäftspartner und Akteure benötigen regelmäßig Zugriff auf Fallakten, Mandantenportale und Recherchequellen. Diesen Zugriff muss eine Kanzlei auf sichere Weise verwalten, überwachen und auch wieder entziehen können. Ohne angemessene Tools dafür riskiert sie Ineffizienzen, Sicherheitslücken und die Verletzung von Compliance-Vorschriften. Gesetze und Branchenstandards zum Datenschutz werden immer strenger. Um Mandantendaten abzusichern und Compliance-Auflagen einzuhalten, ist ein effektives Zugangsdaten- und Zugriffsmanagement für Kanzleien ein Muss.

## In 42 % der Anwaltskanzleien mit 100 oder mehr Mitarbeitern kam es bereits zu einer Datenschutzverletzung.

- American Bar Association

## Sicherer Zugriff, sichere Zugangsdaten – für Anwaltskanzleien essenziell



Als marktführender Anbieter von Lösungen für die Passwort- und Identitätsverwaltung hilft LastPass Anwaltskanzleien, die an sie gestellten Anforderungen der Dokumenten- und Zugriffssicherheit zu erfüllen. LastPass verwahrt sensible Mandantendaten und ermöglicht es Kanzleien, Zugangsdaten unter Wahrung der Vertraulichkeit zu erstellen, zu speichern, freizugeben und zu verwalten. Für Branchen, in denen Diskretion und Vertrauen eine große Rolle spielen, ist LastPass besonders interessant, denn es verwaltet Zugangsdaten zentral und minimiert dadurch das Risiko passwortbezogener Datenschutzverletzungen und unbefugter Zugriffe.



Für Kanzleien gelten strenge Compliance-Auflagen; gleichzeitig müssen sie mit verschiedenen Akteuren in und außerhalb ihres Betriebs möglichst effizient zusammenarbeiten. LastPass wird über eine Cloud-native Plattform ausgeliefert. Sie ermöglicht auf einfache Weise sicheren Zugriff und Datenfreigabe, die Durchsetzung maßgeschneiderter Richtlinien, die Überwachung von Login-Aktivitäten und eine Erstellung detaillierter Berichte zu Audit-zwecken. Kanzleien können damit mühelos die Einhaltung gesetzlicher Vorgaben und Standards nachweisen.



Mit LastPass schützen Kanzleien ihre Mandanten und schaffen Vertrauen. Sie sorgen damit für eine Sicherheit, die ihrer anwaltlichen Sorgfaltspflicht angemessen ist.



# LastPass – viele Vorteile für Anwaltskanzleien

Kanzleien können ihr Sicherheitsrisiko senken, indem sie ihr gesamtes Passwort-Management mit LastPass standardisieren – einfach, kostengünstig und zuverlässig.

<b>Sicherheit</b>	<b>Unbefugten Zugriff verhindern</b>	Anwendungen, Online-Konten, sensible Informationen und Systeme werden vor dem Zugriff Unbefugter geschützt.
	<b>Kontendiebstahl und Datenschutzverletzungen verhindern</b>	Online-Konten und Anwendungen sind zuverlässig verfügbar und zugänglich; Zugangsdaten bleiben stets privat.
	<b>Kontrolle über Schatten-IT</b>	LastPass gibt Überblick und Kontrolle über nicht genehmigte und überschüssige SaaS-Apps, die Freigabe von Zugangsdaten und Verwaltung von Zugriffsrechten. Sicherheitslücken werden aufgezeigt.
	<b>Zugriffsmanagement erweitern</b>	LastPass integriert sich in Identitätsanbieter wie Microsoft Entra und ermöglicht so die Benutzerverwaltung über den ganzen Mitarbeiterlebenszyklus hinweg.
<b>Compliance</b>	<b>Auflagen von Cyberversicherungen einhalten</b>	Cyberversicherungen stellen Anforderungen an die Passwort- und Zugriffsverwaltung – mit LastPass lassen sich diese erfüllen.
	<b>Die Compliance fördern</b>	LastPass ist konform mit Datenschutzgesetzen wie DSGVO, CCPA, GLBA, PCI-DSS, BSA, AML, FCRA und SOX und Sicherheitsstandards wie NIST, CISA, Zero Trust und NERC-CIP.
	<b>Externe Sicherheitsanforderungen einhalten</b>	Robuste Zugriffskontrollen, Regeln für die Freigabe von Passwörtern, starke Authentifizierungsmechanismen und aussagekräftige Berichte unterstützen die Einhaltung der Sicherheitsstandards von Geschäftspartnern.
<b>Effizienz</b>	<b>Eine intuitive Benutzererfahrung bieten</b>	Hunderte anpassbare Richtlinien, eine flexible Rechtevergabe, detaillierte Berichterstattung und verschiedene Authentifizierungsoptionen machen LastPass zu einem unverzichtbaren Baustein im Tech-Stack der Kanzlei.
	<b>Zugriffsmanagement erweitern</b>	Alle Kanzleimitarbeiter können ihre Zugangsdaten auf einfache Weise selbst verwalten.
	<b>Helpdesk entlasten</b>	Probleme mit Zugangsdaten wie vergessenen Passwörtern und Kontoaussperrungen gehen zurück.
<b>Zusammenarbeit</b>	<b>Teamwork durch Freigabe erleichtern</b>	Passwörter und Informationen lassen sich nahtlos und effizient in und außerhalb der Kanzlei freigeben – an Geschäftspartner, Homeoffice-Personal und Auftragnehmer.
	<b>Zügige Akzeptanz und hohe Nutzungsrate</b>	Die komfortable Oberfläche macht die Passwortverwaltung sehr einfach. LastPass wird deshalb schnell angenommen und gerne genutzt.
	<b>Sicherheitskultur entwickeln</b>	LastPass unterstützt Administratoren dabei, eine Sicherheitskultur in der Kanzlei zu verankern und sie vor Datenlecks, Kontendiebstählen und finanziellen Konsequenzen zu schützen.