

WHITEPAPER

Social Media als Unternehmen nutzen:

So schützen Sie die Daten Ihrer Kunden



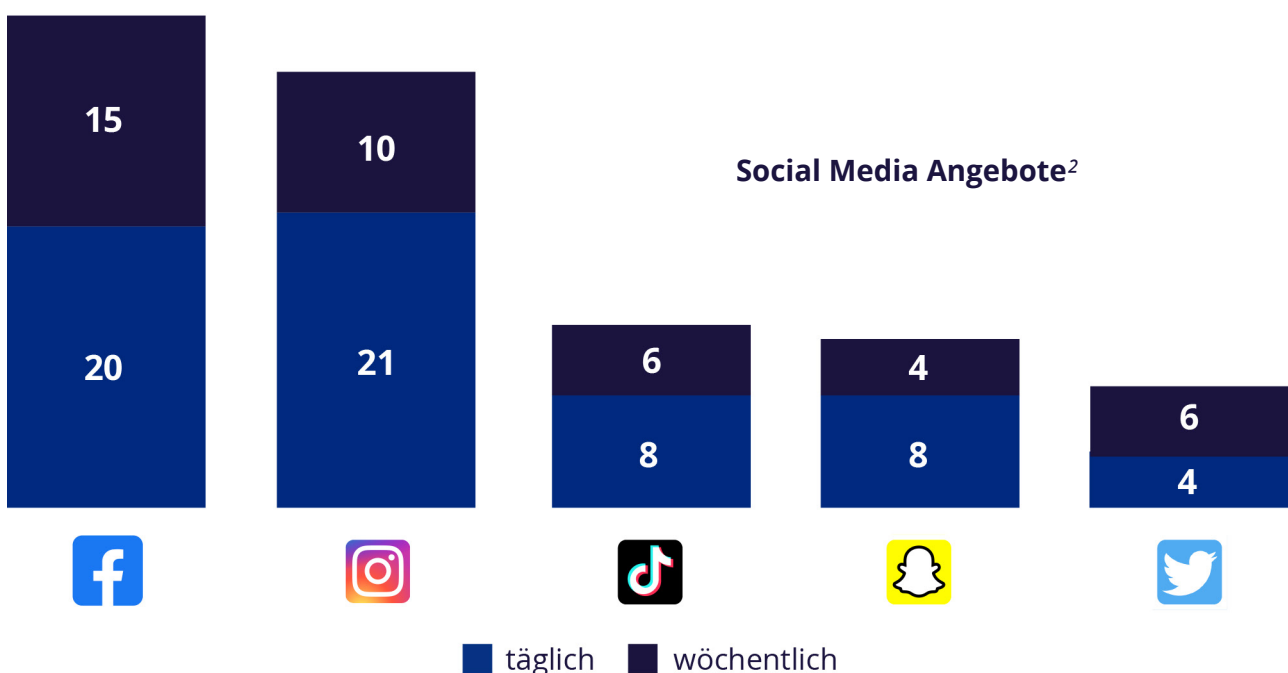
**DATENSCHUTZ
EXPERTE.DE**

Ein Service der Proliance GmbH

Social Media im Unternehmenskontext: Es geht nicht ohne

Ob im beruflichen oder privaten Kontext: Soziale Netzwerke sind für viele Menschen eines der ersten Ziele, wenn sie zum Handy greifen oder mit dem Laptop surfen. Laut aktuellen Erhebungen **nutzen rund 85 Prozent der Deutschen Social Media** und verbringen dort durchschnittlich eine Stunde und 41 Minuten in sozialen Netzwerken.¹

Mit 35 Prozent täglicher oder wöchentlicher Nutzung ist dabei Facebook die Nummer 1 unter den sozialen Netzwerken in Deutschland.



Das ist allerdings nicht der einzige Rekord, den die Plattform hält: 2023 hat der Meta-Konzern, zu dem Angebote wie Facebook, Instagram oder WhatsApp gehören, mit 1,2 Milliarden Euro die **höchste jemals verhängte DSGVO-Strafe** kassiert.

Obwohl diese Summe ein Alarmsignal für alle Unternehmen ist, die Wert auf Datenschutz legen, kommt kaum ein:e Werbetreibende:r an den sozialen Netzwerken vorbei. Wo geteilt, gewischt, vernetzt und gechattet wird, geben Unternehmen inzwischen **mehr als ein Viertel ihrer Werbebudgets** aus.¹

Es spricht nichts dagegen, die Reichweite der sozialen Plattformen zu nutzen. Unternehmen sollten sich jedoch fragen: **Wie können wir Social Media möglichst DSGVO-konform nutzen?** Anhand des Meta-Konzerns, dessen Umgang mit dem Datenschutz immer wieder Schlagzeilen macht, decken wir Gefahren für Ihr Unternehmen auf und zeigen, wie Sie sich und die Daten Ihrer Nutzer:innen bestmöglich absichern.

Quellen:

¹wearesocial.com/de/blog/2023/02/digital-2023-fast-einen-tag-pro-monat-verbringen-die-deutschen-auf-tiktok/

²www.ard-zdf-onlinestudie.de/files/2022/ARD_ZDF_Onlinestudie_2022_Publikationscharts.pdf



Anmerkung

Viele von der Rechtsprechung im Zusammenhang mit Meta entwickelten Grundsätze lassen sich auf alle sozialen Medien übertragen.

Meta und die DSGVO: Beziehungsstatus „Es ist kompliziert“

Seit Inkrafttreten der DSGVO gibt es regelmäßig Diskussionen um den Datenschutz bei Meta. In der folgenden Chronologie fassen wir die wichtigsten Streitpunkte und Rechtsprechungen zusammen.

2018

- Der Europäische Gerichtshof (EuGH) entscheidet: Wenn es um die Einhaltung von DSGVO-Vorgaben geht, liegt eine **gemeinsame datenschutzrechtliche Verantwortlichkeit** des Meta-Konzerns und der auf Plattformen wie Facebook vertretenen Unternehmen vor.
- Bei der Nichtregierungsorganisation für Datenschutz, NOYB (None Of Your Business), gehen Facebook-Beschwerden ein. Hintergrund: Als die DSGVO in Kraft trat, bot Meta kein Opt-in für personalisierte Werbung an, sondern verschob die Einwilligungsklausel in die Allgemeinen Geschäftsbedingungen (AGB). Laut NOYB **umgeht Meta damit die DSGVO**.

2019

- Laut EuGH **verstoßen Social Media Plugins gegen die DSGVO**. Um Plugins wie den „Like-Button“ von Facebook rechtssicher zu nutzen, müssen Unternehmen ihre Nutzer:innen vorab um Erlaubnis bitten.
- Das deutsche Kartellamt untersagt Meta das Sammeln und **Zusammenführen von Nutzer:innendaten** aus verschiedenen Quellen ohne explizite Zustimmung. Es sieht in dieser Praxis einen Datenschutzverstoß und einen **Missbrauch der Marktmacht** des Konzerns.

2021

- Der Bundesdatenschutzbeauftragte Ulrich Kelber fordert die Bundesregierung und die obersten Bundesbehörden auf, ihre **Facebook-Seiten abzuschalten**. Seiner Einschätzung nach können diese **nicht datenschutzkonform betrieben** werden.



2022

- Die unabhängige Datenschutzaufsichtsbehörde des Bundes und der Länder (DSK) **bekräftigt Klebers Einschätzung** in einem Kurzgutachten. Dagmar Hartge, die brandenburgische Datenschutzbeauftragte, fordert daraufhin die obersten Landesbehörden auf, ihre Facebook-Seiten unverzüglich abzuschalten.
- Der Europäische Datenschutzausschuss (EDSA) trifft eine **Entscheidung im NOYB-Streit** und untersagt die DSGVO-Einwilligung in personalisierte Werbung über eine AGB-Klausel.

2023

- Das **Bundespresseamt (BPA) klagt** gegen die Anordnung von Kleber und entscheidet, sie gerichtlich überprüfen zu lassen.
- Zu Beginn des Jahres verhängt die irische Datenschutzbehörde eine Strafe von 390 Millionen Euro gegen Meta, weil der Konzern **beim Targeting DSGVO-Richtlinien missachtet** habe.
- Im Mai verhängt die irische Datenschutzbehörde DPC ein **Rekordbußgeld von 1,2 Milliarden Euro** gegen Meta, weil Daten von Facebook-Nutzer:innen aus der EU auf US-Server übertragen werden. Datenschützer:innen befürchten, dass US-Geheimdienste damit Zugriff auf die Informationen europäischer Nutzer:innen haben.
- Im August kündigt Meta an, die **Rechtsgrundlage** für die „Verarbeitung bestimmter Daten für verhaltensbezogene Werbung“ **zu ändern** und für „bestimmte Daten für verhaltensbezogene Werbung“ die Zustimmung der Nutzer:innen einzuholen. Damit kündigt sich ein Ende des jahrelangen NOYB-Rechtsstreits an.
- Ebenfalls im August untersagt die norwegische Datenschutzaufsicht Meta das Ausspielen personalisierter Werbung für drei Monate – und droht bei Verstößen mit einer Strafe von umgerechnet rund 90.000 Euro pro Tag.



So gehen Facebook & Co. mit Daten um

Das Rekordbußgeld von 2023 und die vorangegangenen Entwicklungen deuten darauf hin, dass sich Meta nicht rechtskonform verhält. Unternehmen mit Accounts bei verschiedenen Meta-Plattformen riskieren deshalb, im Rahmen der gemeinsamen Verantwortlichkeit ebenfalls Verstöße zu begehen.

Diese Gefahr besteht auch bei anderen sozialen Netzwerken. Sie alle sind auf Daten angewiesen, um den Nutzer:innen relevante Inhalte anzuzeigen und sie so lange wie möglich auf der Plattform zu halten. Die Plattformen finanzieren sich über Werbeeinnahmen. Für die Nutzer:innen sind soziale Netzwerke kostenlos – doch oft zahlen sie mit ihrer Privatsphäre.

Facebook und Co. erheben personenbezogene Daten wie Name, Geburtsdatum und Geschlecht. Im Hintergrund sammeln die Plattformen außerdem Daten über das Nutzungsverhalten der User:innen sowie Metadaten, etwa um personalisierte Werbung auszuspielen.

Beispiele für personenbezogene Daten

	Vor- und Nachname		Alter
	Geschlecht		Beruf
	E-Mail-Adresse		Telefonnummer
	amtliche Unterlagen zur Identifikation (die Facebook-Nutzungsbedingungen verlangen, dass Nutzer:Innen zur Registrierung ihren echten Namen verwenden)		

Beispiele für Nutzungsdaten

Nutzungsdaten sind alle Daten, die Nutzer:innen über sich preisgeben, wie Fotos, Interessen und berufliche Informationen. Daraus lässt sich ein umfassendes Persönlichkeitsprofil einer Person erstellen.

Diese Informationen kombiniert Facebook über verschiedene Geräte hinweg, um gezeigte Inhalte wie Werbeanzeigen zu personalisieren.

Beispiele für Metadaten

- IP-Adresse
- Browser
- Betriebssystem
- Standort

Datenschutz bei anderen Social-Media-Plattformen

TikTok gibt Daten an Drittanbieter wie Cloud-Storage-Anbieter weiter und greift unter anderem auf den Standort und den Kalender des Smartphones zu.

Instagram sammelt Informationen wie Aufnahmestandorte und Kontakt- oder Kaufinformationen.

Nach der Umbenennung in X wird Twitter biometrische Daten erfassen sowie die Berufs- und Schulgeschichte der Nutzer:innen. Besonders heikel: Das Unternehmen will die erhobenen Daten für KI-Training nutzen.³



Quellen:

³basicthinking.de/blog/2022/07/18/datenschutz-tiktok-baut-heimlich-server-verbindung-nach-china-auf/
praxistipps.chip.de/tiktok-vs-instagram-wie-aehnlich-sind-sich-die-plattformen_155795
onlinemarketing.de/unternehmensnews/x-user-daten-ki-training-neue-richtlinien



Tipps für eine DSGVO-konforme Social-Media-Nutzung

Die Nutzung von Social-Media-Plattformen wie Facebook ist für Unternehmen aus mehreren Gründen mit Risiken behaftet. Das liegt nicht nur an dem Umgang von Meta mit dem Thema Datenschutz. Gefahren lauern auch auf der Website und den Facebook-Profilen der Unternehmen selbst.

Sie müssen Ihre Kund:innen im Rahmen der Datenschutzerklärung darüber informieren, welche Meta-Werkzeuge Sie auf Ihrer Website nutzen und welche Daten verarbeitet werden. Werkzeuge müssen DSGVO-konform eingebunden sein und dürfen nur mit Einwilligung der Nutzer:innen genutzt werden.

Wichtig ist zudem, in den sozialen Netzwerken DSGVO-konforme Unternehmensprofile zu pflegen. Insbesondere müssen Sie Ihre Informationspflichten aus der DSGVO sowohl im Hinblick auf Ihre eigenen Datenverarbeitungen erfüllen als auch hinsichtlich der Datenverarbeitungen, bei denen Sie gemeinsam mit der Social-Media-Plattform verantwortlich sind.

Ansonsten riskieren Sie, einen Datenschutzverstoß zu begehen und haften als Betreiber einer Facebook-Fanpage für Verarbeitungen, für die Sie verantwortlich sind. Die folgende Übersicht unterstützt Sie dabei, Verstöße gegen die DSGVO zu vermeiden und Ihre Social-Media-Strategie möglichst sicher zu gestalten. Sie erhalten außerdem Tipps für den Einsatz von Werkzeugen wie dem Meta-Pixel.

Tipps 1: Datenschutzerklärung anpassen

Unternehmen sind dazu verpflichtet, Website-Besucher:innen in der Datenschutzerklärung darüber aufzuklären, welche Daten sie mithilfe welcher Werkzeuge verarbeiten. Das gilt auch für Facebook-Unternehmensseiten. darüber aufzuklären, welche Daten sie mithilfe welcher Werkzeuge verarbeiten. Das gilt auch für Facebook-Unternehmensseiten.

1

Verlinken Sie von Ihrem Facebook-Auftritt aus entweder auf eine gesonderte Social-Media-Datenschutzerklärung.

2

Alternativ können Sie direkt auf die Datenschutzerklärung Ihrer Website verlinken und dort in einer gesonderten Passage über die Datenverarbeitung auf Ihrer Facebook-Unternehmensseite informieren.

3

Unsere Empfehlung:

Binden Sie eine separate Datenschutzerklärung auf Ihrer Facebook-Seite ein, die Sie auf das Page Controller Addendum anpassen. Darin können Sie die Verantwortlichkeiten für einzelne Verarbeitungen klären.



Was ist das Page Controller Addendum?

Das Page Controller Addendum ergänzt die Datenschutzbestimmungen von Meta. Es enthält Regelungen zur gemeinsamen Verantwortlichkeit zwischen Unternehmen und Meta und ist eine Reaktion des Konzerns auf das EuGH-Urteil von 2018. Seitdem teilen sich Seitenbetreibende und Meta die datenschutzrechtliche Verantwortung von Fanseiten – das Addendum legt fest, dass alle relevanten Pflichten für den eingeforderten Datenschutz bei Meta liegen.

Konkret heißt das: Betroffenenanfragen wie Löschersuche (Art. 15-20 DSGVO) müssen Unternehmen nur nachkommen, Siehe oben, nach dem Page Controller Addendum muss sich der Fanpage-Betreiber nur dann um solche Ersuchen kümmern, wenn diese nicht die in gemeinsamer Verantwortung durchgeführte Datenverarbeitung betreffen. Das ist zum Beispiel bei Privatnachrichten an Betreibende der Fall.

Wichtige Angaben für Ihre Facebook-Datenschutzerklärung

Ihre Datenschutzerklärung für Facebook sollte alle gem. Art. 13 DSGVO verpflichtenden Informationen enthalten. Insbesondere gehören dazu Angaben

- zu Verantwortlichen der Facebook-Unternehmensseite sowie dessen eigenen Verarbeitungen und Verarbeitungszwecke
- darüber, für welche Verarbeitungen und Zwecke der Betreibende der Unternehmensseite und Meta gemeinsam verantwortlich sind
- zur Rechtsgrundlage für den Einsatz von Facebook Insights. Hier kann auf die vom Nutzer gegenüber Meta abgegebene Einwilligung abgestellt werden
- zur Rechtsgrundlage für die eigenen Datenverarbeitungen
- zu den Kontaktdaten des Datenschutzbeauftragten von Facebook sowie des Betreibenden der Unternehmensseite
- zu einer möglichen Datenweitergabe sowie zu den Empfänger:innen
- zur Datenübermittlung in Drittstaaten und zu geeigneten Garantien
- zu den Rechten der Betroffenen

Setzen Sie zusätzlich auf Ihrer Website Tracking-Tools wie den Meta Pixel ein, ist hierzu ein entsprechender Absatz in die Datenschutzerklärung auf Ihrer Website mit aufzunehmen und sicherzustellen, dass Daten nur an Meta übermittelt werden, nachdem Webseitenbesucher:innen ausdrücklich zugestimmt haben.

Das müssen Sie zur Rechtsgrundlage für die Datenverarbeitung wissen

Facebook holt mittlerweile eine Einwilligung in die Datenverarbeitung ein. Diese bezieht sich ausdrücklich auch auf die Datenweitergabe an Unternehmen, die Facebook Insights im Rahmen der gemeinsamen Verantwortlichkeit nutzen. Diese Einwilligung kann als Rechtsgrundlage angegeben werden.

Unsere Empfehlung: Das durch Facebook zur Einholung der Einwilligung genutzte Cookie-Banner stellt nach unserer ersten Einschätzung wahrscheinlich nicht sicher, dass Einwilligungen tatsächlich wirksam eingeholt werden. Dennoch empfehlen wir die Angabe, dass die Datenverarbeitung im Zusammenhang mit Insights auf Grundlage der von Meta hierzu für die gemeinsamen Verantwortlichen eingeholten Einwilligung nach Art. 6 Abs. 1 S. 1 lit. a DSGVO erfolgt.



Nicht vergessen:

Nehmen Sie Ihre Datenverarbeitung über die Facebook Unternehmensseite in Ihr Verzeichnis der Verarbeitungstätigkeiten auf.

Tipp 2: Impressum bei Facebook korrekt aufsetzen

Um Ihre Informationspflichten gegenüber den Besucher:innen Ihres Facebook-Auftritts gerecht zu werden brauchen Sie neben einer Datenschutzerklärung auch ein Facebook-Impressum. Das Telemediengesetz (TMG) sieht in § 5 eine Impressumspflicht für Facebook vor, da ein Unternehmen die Seite nicht zu privaten oder persönlichen Zwecken betreibt, sondern um den eigenen Umsatz zu steigern.

Insbesondere Konkurrenzunternehmen überprüfen gern, ob Impressum und Datenschutzerklärung ihrer Wettbewerber rechtskonform sind.

Was unbedingt enthalten sein muss, ist:

- Name und Anschrift des Unternehmens
- Kontaktinformationen, die eine schnelle und unkomplizierte Kontaktaufnahme ermöglichen (zum Beispiel Angabe der E-Mail-Adresse)

Darüber hinaus sollte das Impressum leicht zu finden sein. Das OLG München hat diesbezüglich entschieden, dass ein Impressum erst dann leicht erreichbar ist, wenn der Nutzer nicht mehr als zwei Klicks dafür benötigt. Es empfiehlt sich daher, das Impressum im Bereich „Seiteninfo“ unter „Impressum“ einzufügen. Der Name des Betreibers der Webseite und der Facebook-Unternehmensseite sollte dabei übereinstimmen.

Tipp 3: Meta-Pixel sicher einsetzen

Nutzen Sie den Tracking-Pixel für Meta für zielgruppenorientiertes Kampagnenmanagement? Dann liefert Ihnen die folgende Checkliste Empfehlungen, wie Sie ihn Meta Pixel datenschutzkonform nutzen können. Mehr Sicherheit erhalten Sie, wenn Sie die Einstellungen durch einen Datenschutzbeauftragten prüfen lassen.



Sicher werben mit dem Meta Pixel

Wichtige Punkte zum DSGVO-konformen und risikominimierten Einsatz des Meta Pixels auf Ihrer Website

- Basics zu Meta Pixel und Datenschutz
- Datenschutzrelevante Fakten im Überblick
- Die wichtigsten Einstellungen für den Datenschutz

[Jetzt herunterladen](#)

Die Zukunft des Social-Media-Datenschutzes

Meta steht zunehmend unter Druck – nicht nur aufgrund von Milliardenstrafen, sondern durch neue Gesetze wie den **Digital Market Act (DMA)** und den **Digital Service Act (DSA)**. Meta reagiert darauf mit Abo-Plänen: Gegen eine Gebühr sollen Nutzer:innen weniger Werbeanzeigen sehen und gleichzeitig mehr Datenschutz genießen.⁴ Außerdem sollen Meta-Nutzer:innen künftig die Verwendung ihrer Daten für das KI-Modelltraining ablehnen können.⁵ Es gibt jedoch auch Negativentwicklungen wie die Pläne von X, biometrische Nutzer:innendaten zu sammeln.



Was sind DMA und DSA?

Der DMA soll unter anderem die **Marktmacht** großer Plattformen wie Meta begrenzen. Der DSA soll ein besseres und schnelleres Vorgehen **gegen illegale Inhalte** ermöglichen.

Auf Entscheidungen der Social-Media-Anbieter haben Unternehmen keinen Einfluss – sie können aber ihrerseits alles tun, um die **Daten ihrer Kund:innen bestmöglich zu schützen**. Dafür sollten sie die Entwicklungen rund um den Social-Media-Datenschutz regelmäßig verfolgen und gegebenenfalls alle Datenschutzmaßnahmen anpassen, die sie selbst in der Hand haben.

Unsere Tipps dienen dazu, Sie und Ihr Team für die **datenschutzrechtlichen Gefahren** zu sensibilisieren, die von Social-Media-Plattformen ausgehen. Doch selbst wenn alle Schritte befolgt sind, bleibt der Einsatz von Social Media für Unternehmen mit Risiken behaftet.

Um Abmahnungen, Bußgelder und einen Imageverlust zu vermeiden, unterstützen Sie unsere erfahrenen Datenschutzexpert:innen mit ihrer Expertise. Denn neben den genannten Tipps gibt es noch weitere Punkte, die bei der Social-Media-Nutzung in Unternehmen zu beachten sind und unter anderem die Übertragung von Daten an Server in die USA betreffen. Wir beraten Sie gern dazu.

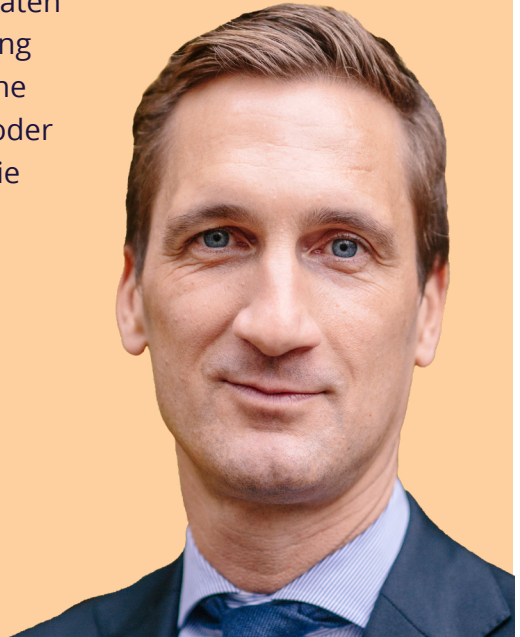
Experten-Kommentar: Deshalb ist Social-Media-Datenschutz wichtig

„Verstöße gegen das Datenschutzrecht können bei einer unbedachten Nutzung von Social Media leicht vorkommen; hier lauern zahlreiche Fallstricke. Eine intensive Auseinandersetzung mit dem Datenschutzrecht und den hieraus erwachsenden Compliance-Vorgaben für Unternehmen ist deshalb unbedingt anzuraten.

Besonderes Augenmerk sollten Unternehmen auf die Impressumspflicht und weitere Informationspflichten legen. Ferner sind die Verarbeitung und Veröffentlichung von Mitarbeiter- und Kundendaten anzugehen, dies gilt insbesondere für die Verwendung von Fotos und Videos. Denn hier drohen empfindliche Bußgelder bis zu einer Höhe von 20 Millionen Euro oder vier Prozent des weltweiten Vorjahresumsatzes sowie darüber hinaus Schadensersatzansprüche der geschädigten Personen.

Nicht zu unterschätzen ist außerdem der damit einhergehende Reputationsschaden.“

Prof. Dr. Boris Paal ist Jura-Professor an der Universität Leipzig und wissenschaftlicher Beirat von Proliance.





Sie haben Fragen? Wir helfen Ihnen weiter!

Sie wünschen eine unverbindliche Beratung zum
Datenschutz Management in Ihrem Unternehmen
und dem Thema externer Datenschutzbeauftragter?

Rufen Sie uns gerne an oder schreiben Sie uns
eine E-Mail!

datenschutzexperte.de
+49 (0)89 2500 392 20
info@datenschutzexperte.de



Alexander Ingelheim
Geschäftsführung

datenschutzexperte.de ist Ihr Partner im Datenschutz.

Wir glauben, dass Datenschutz nicht teuer und komplex sein muss. Mit unseren auf KMU zugeschnittenen Lösungen beraten wir Sie als externer Datenschutzbeauftragter. Alternativ unterstützen wir sowohl interne oder externe Datenschutzbeauftragte mit unserer smarten SaaS-Plattform Proliance 360. So lässt sich Datenschutz einfach & pragmatisch umsetzen. Wir sind ein junges Münchner Unternehmen mit mehr als 70 Mitarbeiter:innen und helfen bereits über 2.000 Unternehmen, die Herausforderungen der DSGVO zu meistern. Sprechen Sie uns gerne an.

Copyright © 2023 PROLIANCE GmbH

Wir behalten uns alle Rechte an diesem Dokument vor. Dieses Whitepaper sowie Teile davon dürfen nicht ohne schriftliche Einwilligung der PROLIANCE GmbH reproduziert oder in kommerzieller Weise verwendet werden. Bitte beachten Sie, dass dieses Whitepaper lediglich einen ersten Überblick über das komplexe Thema Datenschutz für Ihre Website bieten soll und keinesfalls eine Datenschutzberatung ersetzen kann. Trotz höchster Sorgfalt bei der Erstellung des Textes übernehmen wir keine Haftung oder Verantwortung dafür, dass dieser fehlerfrei ist. Dieses Whitepaper ersetzt keine individuelle Rechtsberatung; für eine persönliche Beratung kontaktieren Sie bitte einen unserer Legal Consultants oder einen Rechtsanwalt.



**DATENSCHUTZ
EXPERTE.DE**

Ein Service der Proliance GmbH

Join the movement
Wir sind Mitglied



We take
**Climate
Action**

lfca.earth/co2