



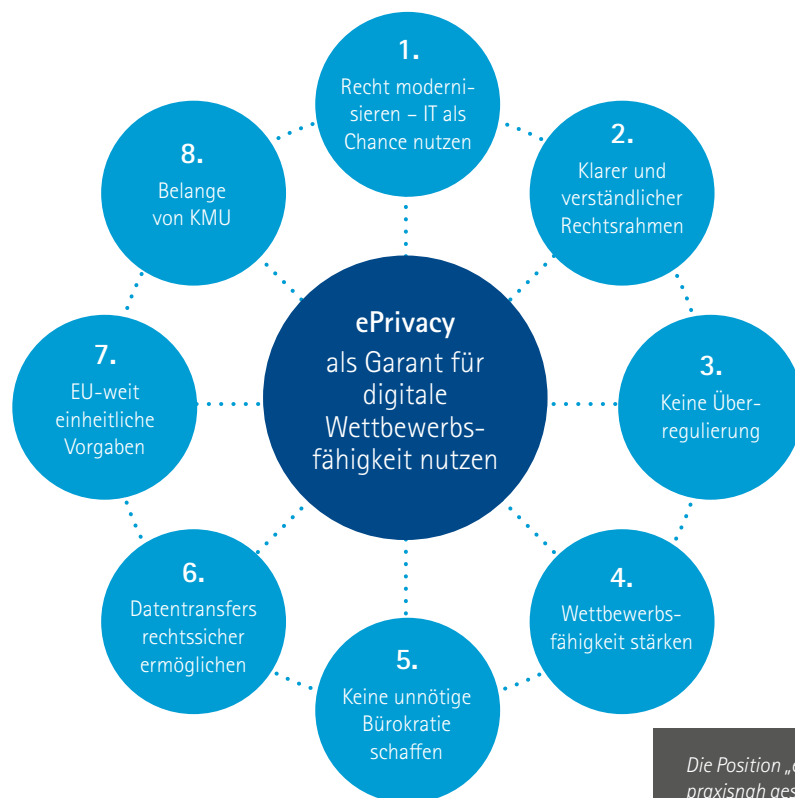
# ePrivacy

## Positionspapier

### ePrivacy modern und praxisnah gestalten – bei TTDSG-Umsetzung nachsteuern

Daten sind ein wertvoller Rohstoff. Für Wissenschaft und Innovationen sind sie ebenso unerlässlich wie für Kommunikation und Wettbewerbsfähigkeit. Europa muss sich zu einer wissensbasierten Datenökonomie entwickeln. Gleichzeitig stellen der Schutz der Privatsphäre und die vertrauliche Nutzung von internetfähigen Endgeräten, d. h. alle mit dem Internet verbindbaren Geräte/Anwendungen, ein hohes Schutzgut dar. Aufgabe des Staates ist es, einen verlässlichen Rechtsrahmen mit klaren, wettbewerbsfähigen, international abgestimmten politischen Rahmenbedingungen vorzugeben, innerhalb dessen die Datenverarbeitung ermöglicht, aber gleichzeitig die berechtigten Schutzinteressen von Bürgern und Unternehmen gesichert werden. Auf EU-Ebene wird aktuell die ePrivacy-Verordnung (ePVo) im Trilog erarbeitet. Mit ihrer Einführung ist frühestens 2024 zu rechnen. Bis dahin gilt in Deutschland das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG). Dieses setzt seit 01.12.2021 Artikel 5 Abs. 3 der ePrivacy-Richtlinie gesamtheitlich um.

Das TTDSG betrifft alle internetfähigen Anwendungen wie z. B. Webseiten, Webanwendungen, Apps, Internet of Things (IoT), Reichweitenmessung und -analyse. Die aktuelle Umsetzung bringt erheblichen finanziellen und personellen Aufwand für die Unternehmen mit sich. Sie schränkt durch eine sehr enge Auslegung der Datenschutzaufsichtsbehörden digitale Gestaltungen im Vergleich zum Ausland erheblich ein. Fehlende Präzisierungen in der Gesetzesbegründung führen zu Unsicherheiten bei der Umsetzung. Um die Wettbewerbsfähigkeit von Deutschland nicht zu gefährden, muss die Auslegung des TTDSG korrigiert werden. Es gilt, Überregulierungen und fortlaufende Anpassungen zu vermeiden, EU-weit einheitliche Rechtsansichten und praxisgerechte Handhabungen anzustreben und digitale Innovationen zu stärken. Gleichzeitig sollten diese Regelungen technologieneutral sowie kohärent und konsistent zu bestehenden Regelungen (z. B. DSGVO) sein. Neue Rechtsentwicklungen (Zahlen mit Daten) und bestehende etablierte Geschäftsmodelle dürfen nicht eingeschränkt werden.



Die Position „ePrivacy modern und praxisnah gestalten bei TTDSG-Umsetzung nachsteuern“ wurde von der IHK-Vollversammlung am 16.03.2022 mit 53 Zustimmungen, 0 Gegenstimmen und 1 Enthaltung beschlossen.



München und  
Oberbayern

## Folgende Anforderungen müssen für TTDSG / ePrivacy gelten

### 1. Recht modernisieren – IT als Chance nutzen

Eine digitale Welt benötigt einen verlässlichen, praktikablen und technikneutralen Rechtsrahmen. Gleichzeitig müssen der Schutz von Privatsphäre und die vertrauliche Nutzung von internetfähigen Endeinrichtungen gewahrt werden. Hier ist die ePrivacy-Gesetzgebung auf Anpassungsbedarf zu prüfen und bei Bedarf zu modernisieren. ePrivacy-Regelungen sollten konsistent und kohärent zu anderen Regelwerken sein wie zur DSGVO und ihren Rechtspflichten (u. a. Pflicht, für Sicherheit nach dem Stand der Technik zu sorgen) oder zum seit Januar 2022 zulässigem Bezahlen mit Daten. Berechtigte Bedürfnisse der Internetwelt müssen rechtlich abgesichert werden. So sollte Werbung User geolokalisiert erreichen können, z. B. unter Einsatz von generischen Informationen der Geo-IP. Die Konferenz der Datenschutzaufsichtsbehörden (DSK) hat sich in ihrer „Orientierungshilfe Telemedien“ nicht geäußert zu „Diensten mit Zusatzfunktion“ bzw. „Zahlen mit Daten“. Hierfür werden praxiskonforme Lösungen benötigt, so dass z. B. die Medienwirtschaft rechtssicher Vertragsmodelle für moderne Informations- und Konsumbedürfnisse anbieten kann.

### 2. Klarer und verständlicher Rechtsrahmen

Der zu schaffende Rechtsrahmen muss klar und verständlich sein. Der Gesetzgeber muss bei Bedarf Umsetzungshinweise über die Erwägungsgründe vorgeben und so selbst für Klarheit sorgen. Keinesfalls sollte die Auslegung allein der DSK obliegen. ePrivacy-Regeln sind nach dem datenschutzrechtlichen Gebot der Transparenz zu formulieren, d. h. in einer klaren und für KMU verständlichen Sprache. Rechtsvorgaben müssen in Praxis Checks vorab geprüft werden, bevor diese in Kraft treten.

### 3. Keine Überregulierung

Die ePVO wird für die Datenverarbeitung mehr Gestaltungsspielräume eröffnen. Mit Blick hierauf sollten in der Übergangszeit Überregulierungen und Anpassungen an wechselnde Rechtsvorgaben und deren Auslegung vermieden werden. Etablierte Techniken und Geschäftsprozesse dürfen grundsätzlich nicht gefährdet werden. Das TCF muss als Standard-Consent-Verfahren erhalten bleiben können. Ein weiteres Aufblähen der Datenschutzregeln muss vermieden werden. Die ePVO sollte die hohen Anforderungen der bisherigen ePrivacy-Richtlinie der EU nicht weiter verschärfen.

### 4. Wettbewerbsfähigkeit stärken

ePrivacy ist ein Marketinginstrument, wenn es zukunftsorientiert und technologieneutral geregelt wird. Gold-Platin-Standards gefährden die Wettbewerbsfähigkeit und müssen sowohl in der Übergangszeit mit Blick auf Deutschland als auch hinsichtlich von ePrivacy im internationalen Vergleich vermieden werden. Forschung und Entwicklung sollen auch künftig in Europa durchführbar und nicht von Abwanderung ins Ausland betroffen sein. So benötigen Unternehmen rechtssichere Verfahren für Kunden-Modelle, um regelmäßig Produktoptimierung anbieten zu können. Daten werden in einer digitalen Gesellschaft in immer neuen Kontexten verarbeitet. Für diese Zweckänderungen benötigt eine wissensgetriebene moderne Wirtschaft belastbare Rechtsgrundlagen. Als solche sieht ePrivacy für die Datenverarbeitung ausschließlich die Einwilligung vor. Gerade bei IoT sollte als Rechtsgrundlage – wie in der DSGVO – auch ein berechtigtes Interesse der Wirtschaft eine Datenverarbeitung legitimieren. Bei „Diensten mit Zusatzfunktion“ und „Zahlen mit Daten“ sollten auch vertragliche Regelungen zulässig sein.

### 5. Keine unnötige Bürokratie schaffen

Staatliche Eingriffe müssen dem Gebot der Wirksamkeit unterliegen. Informations- und Dokumentationspflichten müssen verhältnismäßig sein. Für bestimmte Fallkonstellationen (z. B. fahrendes Fahrzeug) müssen sachgerechte Lösungen für Informationspflichten neu gedacht werden. Neue rechtliche Rahmenbedingungen müssen sachgemäß sein. Anpassungen von Websites, Apps oder IoT verursachen hohen personellen wie finanziellen Aufwand. Diese ziehen zudem eine Anpassung von Datenschutzdokumentationen nach sich. Der Staat darf die Unternehmen nicht mit Kosten, Pflichten und laufenden neuen Anpassungen überfordern. Verpflichtend zu implementierende technische Schutzmaßnahmen müssen zwingend einwilligungsfrei sein. Eine Beurteilung der Erforderlichkeit rein aus Nutzersicht, wie die DSKes in ihrer TTDSG-Orientierungshilfe streng auslegt, greift zu kurz. Berechtigte Belange der Wirtschaft sind hier angemessen zu berücksichtigen.

### 6. Datentransfers rechtssicher ermöglichen

Eine wissensbasierte Datenökonomie kennt keine Grenzen. Daher muss in einer digitalen Welt der Zugriff auf und das Auslesen von Endgeräten geschützt sein und dies unabhängig, ob diese Informationen sich in oder außerhalb von Europa befinden. Weltweit einheitliche Standards hierfür sowie Rechtssicherheit für transatlantische Datentransfers sind insofern unverzichtbar. Benötigt werden staatenübergreifende Vorschriften, die umfassendere Datentransfers ermöglichen als bisherige Rechtsinstrumente wie z. B. Standardvertragsklauseln dies vermögen. Es müssen Brücken zwischen unterschiedlichen Rechtsregimen gebaut werden. Denn die Wirtschaft verlangt einheitliche internationale Standards, nicht viele. Keine Lösung ist ein Umbau von Konzernstrukturen, nur um Rechtsvorgaben anderer Staaten nicht zu verletzen.

### 7. EU-weit einheitliche Vorgaben

Es ist zu begrüßen, dass die ePVO die ePrivacy-Regelungen in der EU vereinheitlichen und harmonisieren wird. Konkretisierungen sollte die ePVO in den Erwägungsgründen enthalten und so direkt für Rechtsklarheit sorgen. Unterschiedliche Auffassungen von Datenschutzaufsichtsbehörden z. B. zu Fragen der Reichweitenmessung sollten spätestens dann vereinheitlicht werden. Wünschenswert wäre bereits jetzt eine zeitnahe Vereinheitlichung von Gesetzesauslegungen. Die ePVO wird Unternehmen mehr rechtlichen Gestaltungsspielraum geben. Insofern sollte diese zeitnah in Kraft treten.

### 8. Belange von KMU

KMU müssen in einer digitalen Welt Waren und Dienstleistungen zunehmend online anbieten. Eine Website rechtssicher zu gestalten, stellt viele Unternehmen mittlerweile vor eine nicht lösbare Herausforderung. Es ist zeitaufwendig und bedarf fachlicher Expertise, eine Datenschutzerklärung rechtskonform zu erstellen. Gerade KMU können sich damit verbundenen hohen finanziellen Aufwand nicht leisten. Eine zweistufige Prüfung nach TTDSG/ePrivacy und nach DSGVO bedarf erklärender und beratender Maßnahmen, um so die Regelungen auch für KMU umsetzbar zu machen. Eine ausschließlich auf eine Einwilligung gestützte Datenverarbeitung nach ePrivacy trifft die KMU besonders hart. Denn große Plattformbetreiber erhalten Einwilligungen viel einfacher als KMU. Insofern sollte die ePVO die Bedürfnisse und die Praxisrealität der KMU stärker berücksichtigen und Erleichterungen bzw. Ausnahmen für KMU vorsehen, um Wettbewerbsverzerrungen zu vermeiden. Zur Umsetzung von Gesetzesvorgaben muss die Wirtschaft angemessene Anpassungsfristen und praxiskonforme Alternativen haben.