Newsletter 09/2026

FOX Group

Online-Portale für Auskunftsersuche gem. Art 15 DSGVO

Damit ein digitales Self-Service-Portal im Unternehmen für Auskunftsersuchende nach Art. 15 DSGVO absolut rechtssicher agiert, müssen fünf Kernkriterien strikt beachtet werden.

An erster Stelle steht die zweifelsfreie Authentifizierung der betroffenen Person: Sensible Daten dürfen erst nach einer sicheren Identitätsprüfung, z.B. per Zwei-Faktor-Authentifizierung, freigegeben werden, um eine Datenpannen zu verhindern. Zudem ist der Schutz Dritter wichtig, weshalb fremde personenbezogene Informationen vor der endgültigen Bereitstellung zuverlässig unkenntlich gemacht werden müssen.

Für die eigentliche Auskunft ist eine durchgehende End-to-End-Verschlüsselung innerhalb des Portals zwingend erforderlich, um unbefugte Zugriffe beim Download sicher auszuschließen. Neben der reinen Datenkopie muss das System auch sämtliche gesetzlichen Metainformationen wie Verarbeitungszwecke, Empfänger und die genaue Speicherdauer übersichtlich bereitstellen. Abschließend darf das bereitgestellte Portal niemals die einzige Option sein. Unternehmen sind rechtlich verpflichtet, den Betroffenen weiterhin alternative, formlose Übermittlungswege wie den Postweg oder klassische E-Mails anzubieten.

Thema 1

Online-Portale für Auskunftsersuche gem. Art 15 DSGVO

Thema 2

Die „Das ist keine KI“-Falle: Warum KI-Entwickler sich beim Datenschutz täuschen

Thema 3

Warum Pflicht-Checkboxen in Datenschutz-erklärungen unnötig sind

Der Versand unserer Informationsbroschüre erfolgt durch Ihre schriftliche Einwilligung. Um diesen abzubestellen, antworten Sie auf die E-Mail mit der Broschüre im Anhang. Alternativ schicken Sie eine E-Mail an info@complimant.de mit Ihrer Bitte um Beendigung.

Die „Das ist keine KI“-Falle: Warum KI-Entwickler sich beim Datenschutz täuschen

Nach diversen Gesprächen mit Unternehmen erkennt man eine Aussage, die sich aus Compliance-Sicht als Irrglaube entpuppt: Weil vieles, was als „KI“ vermarktet wird, in Wahrheit nur aus klassischen Wenn-Dann-Regeln besteht, wiegeln IT-Dienstleister bei der Dokumentationspflicht gerne ab. Der Satz „Das ist eigentlich keine KI“ mutiert gerne zur bequemen Ausrede. Wer jedoch so argumentiert, steht rechtlich schnell mit einem Bein im Bußgeldbereich – besonders dann, wenn das genutzte Tool im Hintergrund via API auf Google Gemini, OpenAI oder Microsoft Copilot zugreift.
Für den Datenschutz und die DSGVO ist es völlig irrelevant, wie „intelligent“ eine Software wirklich ist. Entscheidend ist einzig und allein der Datenfluss. Sobald ein Software-Anbieter im Hintergrund die großen LLM-Anbieter als Unterauftragnehmer einbindet – oder dies über optionale Features einbinden könnte –, greifen harte rechtliche Pflichten.

Viele moderne Software-Suiten integrieren KI-Funktionen standardmäßig als „schlummernde“ Features, die der Nutzer mit einem Klick aktivieren kann. Genau hier greift das Prinzip des „Verantwortlichen“ nach Art. 4 Nr. 7 DSGVO. Das Unternehmen, das die Software für seine geschäftlichen Zwecke bereitstellt, entscheidet über die Mittel der Verarbeitung und trägt die volle rechtliche Verantwortung für den Datenstrom.
Um die Risiken bei solchen Datenströmen zu minimieren, müssen KI-Verantwortliche zwingend spezifische technische und organisatorische Maßnahmen (TOM) implementieren und dokumentiert haben.

Für KI-Verantwortliche bedeutet das: Wenn ein IT-Dienstleister behauptet, ein Tool sei keine KI oder verarbeite ohnehin keine personenbezogenen Daten, sollte dies nicht ungeprüft übernommen werden. Eine solche Verharmlosung deutet möglicherweise darauf hin, dass der Dienstleister sich in der aktuellen Rechtslage nicht auskennt, das muss er auch nicht. Die gesetzliche Haftung für den ungeprüften Datenstrom verbleibt immer beim anwendenden Unternehmen und lässt sich am Ende nicht auf den Dienstleister abwälzen, der nur sein Produkt vermarkten will.

Selbst ein technisch sicherer Aufbau durch starke TOM entbindet weder von der Dokumentationspflicht noch von der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA). KI-Verantwortliche müssen jedes Tool, das personenbezogene Daten an externe Sprachmodelle weiterleitet oder weiterleiten könnte, zwingend in ihr Verzeichnis von Verarbeitungstätigkeiten (VVT) aufnehmen und das damit verbundene Risiko vollumfänglich analysieren. Semantische Wortklauberei schützt im Ernstfall nicht vor Strafe.

Der Versand unserer Informationsbroschüre erfolgt durch Ihre schriftliche Einwilligung. Um diesen abzubestellen, antworten Sie auf die E-Mail mit der Broschüre im Anhang. Alternativ schicken Sie eine E-Mail an info@complimant.de mit Ihrer Bitte um Beendigung.

Warum Pflicht-Checkboxen in Datenschutzerklärungen unnötig sind

Auf zahlreichen Webseiten, insbesondere bei Kontaktformularen, Registrierungsprozessen oder Newsletter-Anmeldungen, begegnen Internetnutzern immer wieder obligatorische Checkboxen mit Formulierungen wie „Ich habe die Datenschutzerklärung gelesen und stimme ihr zu“.

Bei einer klassischen Datenschutzerklärung handelt es sich um eine rein einseitige gesetzliche Informationspflicht des für die jeweilige Datenverarbeitung Verantwortlichen. Gemäß der europäischen Datenschutz-Grundverordnung müssen Webseitenbetreiber lediglich sicherstellen, dass relevante Informationen wie die Identität des Anbieters, die genauen Verarbeitungszwecke, die Rechtsgrundlagen, die geplante Speicherdauer sowie die Betroffenenrechte in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form zur Verfügung gestellt werden. Die Verordnung verlangt an keiner Stelle, dass der betroffene Nutzer diesen Rechtstext tatsächlich liest oder dessen Inhalt aktiv per Mausklick bestätigt.

Im digitalen Online-Kontext reicht es daher vollkommen aus, einen gut sichtbaren Hinweis bereitzustellen, der eine leicht zugängliche, direkte Verlinkung auf das Dokument enthält. Das künstliche Vorschalten von Pflicht-Checkboxen ist nicht nur rechtlich völlig überflüssig, sondern birgt für Unternehmen sogar erhebliche Risiken, da es zu Problemen führen kann. Dies wird dann kritisch, wenn Seitenbetreiber das erzwungene Akzeptieren fälschlicherweise als eine wirksame Einwilligung im Sinne der Datenschutz-Grundverordnung interpretieren. Fehlt es dieser vermeintlichen Einwilligung an der gesetzlich geforderten Freiwilligkeit, Bestimmtheit oder Informiertheit, ist sie rechtlich unwirksam. Dies hat zur Folge, dass der gesamten Datenverarbeitung die notwendige Rechtsgrundlage fehlt.

Auch der Europäische Datenschutzausschuss sieht diesen Umstand kritisch, da er irreführende Formulierungen und intransparente Schaltflächen als klaren Verstoß gegen den übergeordneten Grundsatz der Verarbeitung nach Treu und Glauben einstuft. Nutzer dürfen durch solche Mechanismen nicht im Unklaren darüber gelassen werden, ob sie lediglich eine Information zur Kenntnis nehmen oder zeitgleich eine weitergehende rechtliche Einverständniserklärung abgeben, die das grundlegende Machtverhältnis asymmetrisch verschiebt. Daher ist wichtig zu wissen, dass Webseitenbetreiber auf verwirrende Zustimmungsabfragen verzichten und stattdessen auf eine transparente, gut sichtbare Verlinkung setzen sollten, um rechtliche Fallstricke effektiv zu vermeiden.

Impressum

complimant AG, Edt 4, 84558 Kirchweidach

Vorstand: Franz Obermayer, Ann-Karina Wrede

Vorsitzender des Aufsichtsrates: Christian Volkmer

Telefon: +49 8683 99390-40

E-Mail: info@complimant.de / datenschutz@complimant.de

www.complimant.de

Eintragung im Handelsregister: Amtsgericht: Traunstein

Registernummer: HRB 20500 Steuernummer: 141/120/07009

Umsatzsteuer-Identifikationsnummer gemäß §27a

Umsatzsteuergesetz: DE274380239

Verantwortlich für den Inhalt nach §18 Abs. 2 MStV Franz Obermayer

Der Versand unserer Informationsbroschüre erfolgt durch Ihre schriftliche Einwilligung. Um diesen abzubestellen, antworten Sie auf die E-Mail mit der Broschüre im Anhang. Alternativ schicken Sie eine E-Mail an info@complimant.de mit Ihrer Bitte um Beendigung.