



Damit der Datenschutz nicht zum «Eventkiller» wird

Im Geschäftsumfeld sind Events ein beliebtes Mittel zur Pflege von Beziehungen mit Kunden, Lieferanten oder Mitarbeitenden. Die Bandbreite für Events reicht vom Firmenapéro, der in einem bebilderten Beitrag auf unternehmens-eigenen Social-Media-Kanälen geteilt werden soll, über die Leadgenerierung an Messen bis hin zu Kundenevents. Bei all diesen Events werden regelmässig Personendaten bearbeitet, beispielsweise bei der Einladung über ein spezifisches Tool, der Nutzung der am Event gemachten Bilder im Marketing oder bei der systematischen Nachbearbeitung von Kontaktdaten nach einer Messe.

Damit die Nutzung von Personendaten vor, während oder nach dem Event nicht zu einem rechtlichen Risiko wird, ist es wichtig, dass die zuständigen Entscheidungsträger für die möglichen Gefahren sensibilisiert sind. Besonders im Bereich des Datenschutzrechts bestehen Risiken – nicht zuletzt, weil das Bewusstsein der Eventteilnehmenden für dieses Thema in den letzten Jahren stark zugenommen hat. Bei der Vorbereitung und Durchführung von Events sollte der Datenschutz darum einen Platz erhalten, sodass die rechtlichen und die ggf. damit zusammenhängenden Reputationsrisiken minimiert oder ausgeschlossen werden können. Dadurch können Events weiterhin ohne Frust mit viel Freude und Engagement durchgeführt werden.

Viel Spass bei der Lektüre

Marco S. Meier, RA, MLaw, CIPP/E
Herausgeber

Rechtssicher an Messen Kontakte sammeln

Messen sind für Unternehmen eine der wichtigsten Plattformen, um neue Kunden zu gewinnen, bestehende Geschäftsbeziehungen zu pflegen und das eigene Netzwerk auszubauen. Gerade die Sammlung von Kontaktdaten ist dabei zentral, sei es durch Visitenkarten, digitale Leads, Wettbewerbe oder Newsletter-Anmeldungen. Doch es gelten klare rechtliche Rahmenbedingungen, wie Personendaten erhoben, gespeichert und genutzt werden dürfen.

■ Von Lukas Lezzi

Rechtliche Grundlagen

Gemäss Art. 3 Abs. 1 lit. o Bundesgesetz gegen den unlauteren Wettbewerb (UWG) ist der Versand von elektronischer Werbung per E-Mail grundsätzlich nur in zwei Konstellationen erlaubt:

- mit ausdrücklicher Zustimmung des Empfängers, etwa durch die aktive Anmeldung zu einem Newsletter
- ohne ausdrückliche Zustimmung, wenn bereits eine Kundenbeziehung besteht: Dann hat der Empfänger im Rahmen eines Vertragsabschlusses oder einer Mitgliedschaft seine E-Mail-Adresse freiwillig angegeben, und die Werbung bezieht sich auf ähnliche Produkte oder Dienstleistungen (Werbung an Kunden). Voraussetzung ist jedoch, dass der Empfänger beim Vertragsabschluss oder während der Abwicklung klar und deutlich auf die Möglichkeit hingewiesen wurde, den Erhalt solcher Werbemails abzulehnen, und er diesem nicht widersprochen hat.

Anforderungen an eine wirksame Einwilligung

Damit die Einwilligung zur Bearbeitung von Personendaten, insbesondere für Werbe- und Marketingzwecke, rechtskonform ist, müssen folgende Voraussetzungen erfüllt sein:

- freiwillig:
Die betroffene Person muss ihre Zustimmung ohne Zwang erteilen

können. Eine Einwilligung ist unwirksam, wenn sie an Bedingungen geknüpft wird, die für die Leistung nicht notwendig sind.

- informiert:
Vor Abgabe der Einwilligung muss klar und verständlich darüber informiert werden, welche Daten erhoben werden, zu welchem Zweck sie bearbeitet werden (z. B. Zusendung von Produktinformationen, Einladungen zu Veranstaltungen), wer Empfänger der Daten ist und welche Rechte die betroffene Person hat (Auskunft, Berichtigung, Löschung, Widerruf). Diese Informationen können im Formular selbst kurz dargestellt und mit einem Hinweis auf eine ausführliche Datenschutzerklärung (z. B. per QR-Code oder Link) ergänzt werden.
- Nachweisbarkeit:
Das Unternehmen muss jederzeit belegen können, dass eine wirksame Einwilligung erteilt wurde. Deshalb sollte dokumentiert werden, wann, wie und wofür die Einwilligung eingeholt wurde. Bei digitalen Formularen geschieht dies in der Regel durch Protokollierung (Zeitstempel, IP-Adresse, verwendetes Endgerät).
- Widerrufbarkeit:
Die Einwilligung darf nicht «unumkehrbar» sein. Jede betroffene Person muss ihre Zustimmung jederzeit und ohne Nachteile widerrufen können.

PRAXISTIPP



Praktische Tipps für den Messealltag

- Visitenkarten: Das Überreichen einer Visitenkarte erlaubt nur die persönliche Kontaktaufnahme. Für Marketing oder Newsletter braucht es eine separate Zustimmung.
- Newsletter Anmeldeformular: Das Formular muss eine klare Checkbox für die Newsletter-Einwilligung enthalten, die nicht vorab angekreuzt sein darf, da sie aktiv vom Besucher angewählt werden muss. So ist die Zustimmung eindeutig, freiwillig und dokumentiert.
- Datenschutzerklärung: Da bei einem E-Mail-Newsletter Personendaten bearbeitet werden, muss beim Anmeldeformular ein Hinweis auf die Datenschutzerklärung (meist als Link) zu finden sein. Es bedarf jedoch keiner Einwilligung in die Datenschutzerklärung.
- digitale Tools: Lead-Apps erleichtern die Erfassung von Messekontakten. Sie speichern nicht nur die Kontaktdaten, sondern auch die Einwilligung mit Zeitstempel.
- Wettbewerb: Bei Gewinnspielen dürfen die Daten nur für die Abwicklung genutzt werden. Wer zusätzlich Marketing erhalten möchte, muss das separat ankreuzen.

nen. Praktisch bedeutet das: Jeder Newsletter muss einen funktionierenden Abmeldelink enthalten, und Anfragen auf Löschung oder Abmeldung sind unverzüglich umzusetzen.

Wie dürfen Personendaten gesammelt werden?

Visitenkarten

Das Überreichen einer Visitenkarte ist ein konkludentes Einverständnis, dass die Daten zur Kontaktaufnahme im Kontext des übergebenen Zwecks genutzt werden dürfen (z. B. persönlicher Follow-up).

Das Überreichen einer Visitenkarte bedeutet aber nicht automatisch, dass die regelmässige, automatisierte Nutzung für Marketing (z. B. Newsletter) erlaubt ist, weil dafür eine separate, ausdrückliche Einwilligung (Opt-in) nötig ist.

Digitale Erfassung (Lead-Apps, QR-Codes)

Viele Messen bieten digitale Tools wie QR-Codes und Leads-Apps an, mit denen Besucher ihre Daten scannen lassen können. Im QR-Code des Besuchers (auf dem Batch oder der Eintrittskarte) sind seine Kontaktdaten hinterlegt (z. B. Name, Firma, E-Mail-Adresse). Aussteller nutzen eine Lead-App, die diese Codes scannt und die Daten in einer strukturierten Form speichert und für das Nachfassen aufarbeitet. Statt Visitenkarten in Stapeln zu sammeln oder handschriftliche Listen zu führen, ermöglicht eine Lead-App eine schnelle, papierlose und rechtssichere Datenerfassung.

Bei der Nutzung von Lead-Apps sind folgende Punkte zu beachten:

- Vor dem Scan muss klar kommuniziert werden, zu welchem Zweck die Daten bearbeitet werden.
- Der Links zur Datenschutzerklärung muss angezeigt werden.
- Der Empfänger kann die Einwilligung durch aktives Ankreuzen eines entsprechenden Kästchens (sog. Checkbox) oder durch das Angeben der E-Mail-Adresse bei einem separaten Newsletter-Anmeldeformular geben («Opt-in»). In was der Empfänger einwilligt, muss für ihn klar ersichtlich sein. Daher muss eine kurze Beschreibung bzw. ein Einwilligungstext vorliegen.
- Um den Nachweis zu sichern und Missbrauch auszuschliessen, ist ein Double-Opt-in-Verfahren empfehlenswert. Dabei erhält der Interessent nach der Anmeldung eine Bestätigungs-E-Mail, in der er den Eintrag nochmals durch Anklicken eines Links bestätigt. Erst nach dieser Bestätigung darf die Adresse aktiv für den Versand genutzt werden.
- Die Zustimmung muss protokolliert werden (Zeitpunkt, Quelle, Device). Dies dient als Nachweis.

Gewinnspiele und Wettbewerbe

Gewinnspiele sind ein beliebtes Instrument zur Lead-Generierung, bergen aber datenschutzrechtliche Risiken.

CHECKLISTE



Jedes Unternehmen muss sich mit Cyberrisiken befassen.

Dos:

- Einwilligung einholen: Klare Checkbox mit aktivem Anklicken und Double-Opt-in mit Bestätigungs-E-Mail nutzen.
- Transparenz schaffen: Kurzinfo, zu welchem Zweck die Personendaten bearbeitet werden, und Link zur Datenschutzerklärung.
- Visitenkarten richtig nutzen: nur für Follow-up, nicht für Newsletter ohne Opt-in.
- Wettbewerbe trennen: Neben der Teilnahme eine separate Checkbox zur Newsletter-Anmeldung aufschalten.
- Daten schützen: Zugriff beschränken, Daten verschlüsseln, Löschkonzept implementieren.

Don'ts:

- Keine unbefristete Speicherung von Leads ohne Zweck.
- Keine Kopplung von Teilnahme am Wettbewerb und Werbung.
- Keine versteckten Klauseln bei der Einwilligung zum Werbe-Newsletter. Unzulässig ist z. B. ein Hinweis zur Newsletter-Anmeldung im Fliesstext der Teilnahmebedingungen eines Gewinnspiels, ohne separate Checkbox.

Die im Rahmen eines Wettbewerbs erhobenen Daten dürfen nur für die Durchführung und Abwicklung des Gewinnspiels genutzt werden (z. B. Benachrichtigung der Gewinner). Soll darüber hinaus eine Nutzung für Marketing oder Newsletter erfolgen, ist eine separate und ausdrückliche Einwilligung erforderlich. Es müssen daher folgende Punkte berücksichtigt werden:

- keine Kopplung: Die Teilnahme am Gewinnspiel darf nicht von der Einwilligung in Werbung abhängig gemacht werden («Kopplungsverbot»). Wer nur am Wettbewerb teilnehmen möchte, darf nicht gezwungen werden, gleichzeitig den Newsletter zu abonnieren.
- Transparenz: Die Einwilligung muss klar erkennbar, freiwillig und aktiv erfolgen (z. B. über eine eigene, deutlich sichtbare Checkbox). Hinweise im «Kleingedruckten» oder in

schwer verständlichen Formulierungen sind unzulässig.

In der Praxis heisst dies, neben dem Pflichtfeld für die Wettbewerbsteilnahme (Name, E-Mail zur Gewinnbenachrichtigung) soll eine separate Checkbox für Werbung angebracht sein, welche z.B. wie folgt lautet: «Ja, ich möchte künftig per E-Mail über Produkte und Angebote der XY AG informiert werden. Ich kann meine Einwilligung jederzeit widerrufen.» So sind Wettbewerb und Marketing klar voneinander getrennt, und die Datenverwendung bleibt rechtssicher.

Sicherheit der gespeicherten Daten

Bei der Speicherung der Kontaktdaten ist auf angemessene technische und organisatorische Massnahmen zu achten.

- Es muss sichergestellt werden, dass nur befugtes Personal Zugang zu jenen Personendaten hat, die für die Erfüllung seiner Aufgaben erforderlich sind (Need-to-know-Prinzip).
- Personendaten sollen verschlüsselt werden (z. B. durch Passwortschutz).
- Der Aussteller muss die Einhaltung der Rechte der betroffenen Personen sicherstellen können.
- Daten dürfen nur so lange gespeichert werden, wie sie zur Erfüllung

des Zwecks gebraucht werden, das heisst, es muss ein Löschkonzept implementiert und umgesetzt werden.

- Falls Dritte Zugriff auf die Personendaten haben, muss ein Auftragsbearbeitungsvertrag abgeschlossen werden.
- Es sind Prozesse und Ressourcen einzusetzen, um Datenschutzverletzungen zu erkennen, abzumildern, zu behandeln, zu melden und daraus zu lernen.

Speicherung und Löschung der Personendaten

Gesammelte Kontakte dürfen nur so lange gespeichert werden, wie es für den Zweck notwendig ist. Alte oder inaktive Leads sollten regelmässig gelöscht werden. Wenn jemand am Stand seine Daten hinterlässt, ist der erkennbare Zweck meistens die Kontaktaufnahme und Information über Produkte/Dienstleistungen. Das heisst, es ist ein Follow-up nach der Messe gedeckt. Wenn die Person nicht reagiert oder kein Interesse signalisiert, müssen ihre Kontaktdaten nach angemessener Zeit gelöscht oder anonymisiert werden. Hier empfiehlt es sich, nach sechs bis zwölf Monaten zu prüfen, ob noch ein berechtigtes Interesse besteht, ansonsten müssen die Daten gelöscht bzw. in ein Archiv mit

eingeschränktem Zugriff verschoben werden.

Hat der Besucher hingegen aktiv zum Erhalt des Newsletters zugestimmt, dürfen seine Daten bis auf Widerruf der Einwilligung bearbeitet werden. Doch auch bei Einwilligungen gilt, dass die Daten aktuell und richtig sein müssen (Art. 6 Abs. 5 DSG). Wenn eine Adresse lange nicht mehr genutzt wird (z. B. Bounces [fehlgeschlagene E-Mail-Zustellung]), sollte sie bereinigt oder gelöscht werden.

Fazit

Das Sammeln von Kontakten auf Messen ist möglich, erfordert aber klare Strukturen und Transparenz. Entscheidend ist, dass Interessenten genau wissen, wofür ihre Daten verwendet werden, und dass das Unternehmen Einwilligungen zum Versand von Werbe-Newslettern von den betroffenen Personen aktiv einholt und entsprechend dokumentiert.

AUTOR



Lukas Lezzi ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.

DATENSCHUTZ



WEKA Praxis-Seminar

Künstliche Intelligenz (KI) und Datenschutz

KI im Unternehmen datenschutzkonform nutzen und einsetzen



So setzen Sie KI-Tools nach den Vorgaben des Datenschutzes rechtssicher im Unternehmen ein

In diesem praxisorientierten Workshop erhalten Sie einen fundierten Überblick über die aktuellen rechtlichen Anforderungen an KI-Systeme (bspw. ChatGPT, Perplexity, Gemini oder Open Source Modelle) im Unternehmen. Anhand konkreter Beispiele und Übungen lernen Sie, wie Sie typische Datenschutzrisiken erkennen, bewerten und vermeiden können – von der korrekten Datenschutz-Folgenabschätzung bis zur Vermeidung von möglichen Haftungsfolgen.

Nächste Termine

- Mittwoch, 12. November 2025
- Mittwoch, 25. März 2026
- Donnerstag, 3. September 2026

Dauer und Ort: 1 Tag, 09:00–16:30 Uhr
Zürich, Zentrum für Weiterbildung
der Uni Zürich

Seminarleitung: Florian Müller

Jetzt informieren und anmelden:

www.praxisseminare.ch oder Telefon 044 434 88 34