GDMA GLOBAL PRIVACY PRINCIPLES

(Übersetzung der englischen Originalfassung, die auf der Webseite der Global DMA abrufbar ist)

PRÄAMBEL

Neue Technologien und die Nutzung persönlicher Daten öffnen der Menschheit die Möglichkeit zu einem besseren und nachhaltigeren Leben und Konsumverhalten. Daten spielen dabei eine immer größere Rolle. Der Nutzen von Daten für Gesellschaft und Wirtschaft lässt sich nur durch einen zuverlässigen und vertrauensvollen Umgang mit diesen erreichen. Grundsätze für Privatsphäre und Datenschutz tragen dazu bei und bilden gleichzeitig den Rahmen für einen verantwortungsvollen freien Informationsfluss auf der ganzen Welt.

Die GDMA Global Privacy Principles schaffen einen weltweit passenden Rahmen für die Kundenkommunikation, der alle rechtlichen und kommerziellen Ansätze abdecken soll. Sie sind als Best Practice Instrument konzipiert und sollen als Leitfaden für Selbstregulierung und Gesetzgebung dienen.

Die GDMA Global Privacy Principles stellen eine ambitionierte Verpflichtung für Unternehmen, Regierungen und Menschen dar. Sie zielen darauf, vertrauenswürdiges und erfolgreiches wirtschaftliches Handeln zu kultivieren, indem sie jedem Einzelnen mit Fairness, Transparenz und Respekt vor der Privatsphäre zur Seite stehen. Das Leitprinzip des Respekts und der Achtung der Privatsphäre erzeugt Vertrauen innerhalb der Kundenkommunikation – im Sinne des Austauschs von Werten zwischen einer erfolgsorientierten Organisation und einem an Nutzen interessierten Individuum. Die Prinzipien stellen sicher, dass Unternehmen auf der ganzen Welt das Individuum in den Mittelpunkt ihres Handelns stellen, damit ihnen Vertrauen und Respekt entgegengebracht werden und sie in einer globalisierten Welt überall Bestand haben.

PRINZIPIEN

1. Achten Sie die Privatsphäre !

Die Erwartungen des Einzelnen an den Datenschutz zu respektieren und wertzuschätzen, ist entscheidend für das Vertrauen in wirtschaftliches Handeln. Unternehmen müssen betroffenen Personen helfen, sich im Rahmen der Marketingaktivitäten sicher und wohl zu fühlen (z. B. beim Surfen im Internet, beim Empfang einer E-Mail, bei der Nutzung einer mobilen App

oder beim On- und Offline-Kauf). Das wiederum zahlt sich aus – für die betroffenen Personen durch vertrauensvolle Kommunikation und für die Unternehmen durch weltweite Wertschöpfung.

Umsetzung

- Unternehmen müssen Datenschutz durch Kodizes oder Richtlinien zu einem wesentlichen Element der Unternehmenskultur machen, das vom Top-Management vorgelebt und an alle Beteiligten kommuniziert wird.

- Unternehmen haben Maßnahmen zu ergreifen, um sicherzustellen, dass Mitarbeiter, Partner und Lieferanten ihre Datenschutz-Policy verstehen und diese mittragen.

- Mitarbeiter sind zu schulen und zu verpflichten, den Datenschutz zu respektieren und die Datensicherheit zu gewährleisten.

- Unternehmen sollten einen "Privacy by Design"-Ansatz verfolgen.

2. Kommunizieren Sie klar und transparent !

Unternehmen müssen Vertrauen aufbauen und pflegen, indem sie gegenüber betroffenen Personen klar und transparent über die Erhebung, Verwendung und Weitergabe personenbezogener Daten aufklären.

Umsetzung

Erheben Unternehmen personenbezogene Daten, sind folgende Informationen (in Datenschutz-Policies und darüber hinaus) rechtzeitig, leicht zugänglich und klar bereitzustellen:

- Die Identität des Unternehmens,

- welche personenbezogenen Daten erhoben und wie diese genutzt werden sollen,

- der Zweck der Verarbeitung personenbezogener Daten.

- Ist geplant, personenbezogene Daten weiterzugeben, auf welche Weise und an welche Art von Unternehmen.

- Das Recht des Betroffenen auf Berichtigung, Aktualisierung und Löschung bzw. Sperrung seiner personenbezogenen Daten sowie auf deren Zugang gemäß der jeweils regional geltenden Gesetze. Dies umfasst auch die Information darüber, wie diese Rechte ausgeübt werden können.

- Die verständliche Erklärung des Umgangs mit den Daten sowie etwaige Kosten, die betroffenen Personen entstehen können.

- Die Quellen der Daten, sofern diese nicht direkt von der Person erhoben wurden.

3. Respektieren Sie persönliche Einstellungen und Wünsche !

Unternehmen müssen die Wünsche und Vorgaben des Einzelnen in Bezug auf die Verwendung seiner Daten in der Marketingkommunikation beachten, wann immer dies

rechtlich und technisch möglich ist. Es dient einer effizienteren Kommunikation, von der sowohl der Einzelne als auch die Unternehmen profitieren.

Umsetzung

- Jedes Unternehmen muss betroffenen Personen eine einfache Möglichkeit bieten, ihren jeweiligen Wunsch bezüglich des Erhalts/Nichterhalts von Informationen durch das Unternehmen festzulegen.

- Dies gilt auch bezüglich möglicher Widerspruchsmöglichkeiten (Preference Services), die staatlicherseits oder durch die Privatwirtschaft zur Verfügung gestellt werden.

- Unternehmen haben sicherzustellen, dass betroffenen Personen verständlich kommuniziert wird, was opt-in/opt-out/Widerspruch etc. insbesondere für die daraus resultierende Verarbeitung ihrer Daten bedeuten.

4. Handeln Sie maßvoll und ethisch vertretbar !

Die ordnungsgemäße Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten ist für die Integrität des digitalen Marketings von entscheidender Bedeutung. Besondere Vorsicht gilt beim Umgang mit sensiblen Daten.

Umsetzung

- Unternehmen müssen die Erhebung personenbezogener Daten auf das zur Erfüllung ihres legitimen Zwecks Erforderliche beschränken.

- Unternehmen dürfen personenbezogene Daten nicht für Zwecke verwenden oder offenlegen, die über den ursprünglichen Erhebungsgrund hinausgehen.

- Unternehmen sollten personenbezogene Daten sicher und nur so lange speichern, wie es der mitgeteilte Zweck erfordert.

- Unternehmen sollten besonders sorgfältig im Umgang mit solchen personenbezogenen Daten sein, die bei falscher Handhabung Personen schaden können.

- Werden personenbezogene Daten über Kinder erhoben, ist sicherzustellen, dass alle erforderlichen Informationen für das Kind verständlich sind und einem Elternteil oder den Erziehungsberechtigten zur Verfügung gestellt werden.

5. Übernehmen Sie die Verantwortung !

Unternehmen sind für personenbezogene Daten verantwortlich, die sie zur Durchführung von Marketingaktivitäten nutzen, auch wenn diese an Dritte (Auftragsverarbeiter) übertragen oder abgetreten werden.

Umsetzung

- Unternehmen müssen gewährleisten, dass ihre mit dem Umgang mit personenbezogenen Daten und mit Marketingaktivitäten betrauten Mitarbeiter die Belange der Privatsphäre und des Datenschutzes beachten.

- Jede Führungskraft im Unternehmen ist dafür verantwortlich, dass innerhalb ihres Einflussbereichs personenbezogene Daten bei allen Tätigkeiten und Abläufen verantwortungsvoll verwendet werden.

- Unternehmen sollten regelmäßig interne Datenschutz-Schulungen für alle Mitarbeiter durchführen, die personenbezogene Daten verarbeiten.

- Unternehmen haben regelmäßig Audits über den Umgang mit personenbezogenen Daten durchzuführen und zu dokumentieren.

-Beauftragen Unternehmen Dritte mit der Verarbeitung von Daten, müssen sie sicherstellen, dass auch diese gleichermaßen die Privatsphäre und den Datenschutz beachten.

6. Schützen Sie Daten vor unbefugtem Zugriff !

Unternehmen haben die notwendigen technischen und organisatorischen Maßnahmen zu treffen, um personenbezogene Daten vor unbefugtem Zugriff, Veränderung, Missbrauch, Offenlegung oder Verlust zu schützen.

Umsetzung

- Richtlinien zur Informationssicherheit sind schriftlich festzuhalten und in die Praxis umzusetzen. Dazu gehören periodisches Überprüfen sowie regelmäßige Kontrollen und Tests der technischen Systeme, die personenbezogene Informationen verarbeiten.

- Unternehmen müssen den Zugang zu ihren Systemen auf das „Need-to-know“-Prinzip beschränken. Jeder Benutzer sollte nur Zugriff auf die zur Erfüllung seiner Aufgaben benötigten personenbezogenen Daten haben.

- Wann immer möglich, sollte eine Verschlüsselung und/oder Pseudonymisierung zum Schutz personenbezogener Daten erfolgen. Dies gilt insbesondere für die Übertragung oder Speicherung in mobilen oder portablen Geräten.

- Unternehmen sollten bei der Entscheidung über einzurichtende Sicherheitsmaßnahmen einen risikobasierten Ansatz zugrunde legen und sicherstellen, dass potenziell kritische personenbezogene Daten ein höheres Sicherheitsniveau und erweiterte Zugriffsbeschränkungen erhalten.

- Erhebliche Sicherheitsverletzungen sind unverzüglich den zuständigen Aufsichtsbehörden sowie den jeweils Betroffenen zu melden. Zudem ist sicherzustellen, dass personenbezogene Daten nach einem Verlust, unbefugten Zugriff oder einer unberechtigten Offenlegung wieder gesichert und geschützt werden.

7. Dokumentieren Sie Ihre Maßnahmen nachweisbar !

Unternehmen müssen nachweisen, dass sie entsprechend der hier beschriebenen Grundsätze die notwendigen internen Vorgaben für einen verantwortungsvollen Umgang mit von ihnen verarbeiteten personenbezogenen Daten getroffen und umgesetzt haben.

Umsetzung

Um Verantwortlichkeit zu zeigen sind Unternehmen verpflichtet,

- ein umfassendes Datenschutzkonzept vorzuhalten,

- dieses bei Bedarf nachzuweisen, insbesondere auf Verlangen einer Datenschutzbehörde.

- mit einer klaren, frei zugänglichen Datenschutzerklärung ihre Verpflichtung zur Einhaltung der genannten Prinzipien darzulegen,

- durch entsprechende Aufzeichnungen/Dokumentationen die Einhaltung dieser Grundsätze nachzuweisen.

- ein geeignetes System zur Überwachung und Prüfung einzuführen.

- interne organisatorische Maßnahmen zu ergreifen, die gewährleisten, dass sich die Mitarbeiter und Mitarbeiterinnen verantwortungsvoll gemäß den festgelegten Grundsätzen verhalten.

Definitionen

1. Einzelperson: Die jeweils betroffene Person, d. h. eine natürliche Person, die direkt oder indirekt mit vertretbarem Aufwand identifiziert werden kann. Dazu zählen insbesondere die Zuordnung zu einer Kennung wie einem Namen, einer ID-Nummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

2. Unternehmen: Die Adressaten der Global Privacy Principles, die also personenbezogene Daten für sich oder im Auftrag (z. B. Cloud-Dienste, Contact-Center, Outsourcing-Unternehmen) erheben und mit diesen umgehen.

3. Datenschutz-Policy/Datenschutzhinweis: Die klare und umfassende Vorgabe für den Datenumgang innerhalb eines Unternehmens. Sie schließt die Art und Weise mit ein, wie das Unternehmen Daten erhebt, verwendet, speichert und weitergibt sowie Informationen über die Rechte der Einzelperson in Bezug auf den Schutz ihrer Daten. Darüber hinaus beschreibt die Datenschutz-Policy, wie vorzugehen ist, wenn eine Person sich in ihren Datenschutzrechten verletzt sieht.

4. Personenbezogene Daten: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (Individuum) beziehen.

5. Verarbeitung personenbezogener Daten: Jede Handlung, die mit personenbezogenen Daten vorgenommen wird. Sie reicht von Erhebung, Aufzeichnung, Organisation, Strukturierung, Speicherung, Anpassung oder Veränderung, Abruf, Abfrage, Nutzung, Offenlegung durch Übermittlung, Verbreitung oder sonstige Bereitstellung, Abgleich oder Verknüpfung, Einschränkung bis zu Löschung oder Zerstörung.

6. Sensible personenbezogene Daten: Personenbezogene Daten, die zu einer Ausgrenzung der Person führen und/oder der Person schaden können, wenn sie ohne Zustimmung veröffentlicht werden und Unbefugte auf sie zugreifen. Beispiele: Rassische

oder ethnische Herkunft, sexuelle Orientierung, politische Meinung, religiöse oder philosophische Überzeugung oder Zugehörigkeit. Daten, die sich auf Minderjährige beziehen, können ebenfalls sensibel sein.

7. Privacy by Design: Ein Prinzip, das von jedem Unternehmen verlangt, schon im Voraus die Auswirkungen auf die Privatsphäre zu berücksichtigen, sobald ein Marketingprodukt, eine Dienstleistung oder ein bestimmtes Verfahren konzipiert wird. Frühes Einbeziehen möglicher Einflussfaktoren sowie die Entwicklung und Integration von Datenschutzlösungen in der Startphase eines Projekts helfen, etwaige Probleme im Vorfeld zu erkennen und zu lösen.

8. Verschlüsselung: Die Umwandlung von Informationen oder Daten in einen Code, um unbefugten Zugriff zu verhindern. Sie kommt häufig bei Texten, Nachrichten, Dokumenten Bildern oder Daten zum Einsatz, um Informationen für solche Personen und/oder Unternehmen unlesbar zu machen, die nicht im Besitz des Entschlüsselungscodes sind.

9. Pseudonymisierung: Der Prozess, bei dem personenbezogene Daten mit einem Namen, einem Begriff oder einer Beschreibung versehen werden, der/die sich von der tatsächlichen Identität einer Person unterscheidet. Dadurch können personenbezogene Daten ohne Verwendung zusätzlicher Informationen nicht mehr einer bestimmten Person zugeordnet werden.

10. Verletzung des Schutzes personenbezogener Daten: Eine Verletzung der Sicherheit, die zur versehentlichen oder unrechtmäßigen Zerstörung, zum Verlust, Diebstahl, zur Änderung, zum unbefugten Zugriff auf oder zur Offenlegung von personenbezogenen Daten führt.

Mai 2021
