ADEX

DSGVO Maßnahmen Plan

The ADEX hat mit dem Datenschutzbeauftragten folgenden Maßnahmenplan zur Erfüllung der am 25. Mai 2018 in Kraft tretenden europäischen Datenschutzgrundverordnung (DSGVO) und des neuen deutschen Bundesdatenschutzgesetz (BDSG-neu) erarbeitet.

Die Verarbeitung von personenbezogenen Daten ist nur zulässig, wenn eine Einwilligung der betroffenen Person vorliegt oder das Gesetz eine Datenverarbeitung gestattet (sogenannter Erlaubnistatbestand).

Neu sind aber die Erlaubnistatbestände im Art 6 DSGVO. Insbesondere **Art. 6 Abs. 1f DSGVO** enthält eine für die Praxis weitreichende und zum Teil neue Regelung. Danach ist die Verarbeitung von personenbezogenen Daten auch ohne ausdrückliche Einwilligung zulässig, wenn die Verarbeitung zur Wahrung der „berechtigten Interessen" des Verantwortlichen (des Werbetreibenden) oder eines Dritten (z. B. eines Kooperationspartners) erforderlich ist, sofern nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Auch die Interessen der Werbeindustrie können ein berechtigtes Interesse darstellen. Sie sind damit nicht von vorneherein weniger wert, als die Interessen der Betroffenen, etwa die Besucher einer Website.

- Überarbeitung der **Datenschutzerklärung**, insbesondere um die neuen Informationspflichten zu erfüllen und die Nutzer über ihre neuen Rechte zu belehren. Insoweit wird in der Erklärung die Cookie-Kennung angezeigt und ein Kontaktformular eingebunden, das diese Kennung bei Anfragen der Nutzer übermittelt. Über die Datenschutzerklärung wird der Nutzer sein/e Cookie/s löschen und einem Tracking widersprechen können (durch Setzen eines Cookies ohne Kennung oder durch Verwendung des Do-Not-Track-Headers, welche dem Nutzer erläutert wird). Im Übrigen wird der Nutzer seine Rechte über das Kontaktformular bzw. per E-Mail geltend machen können (Auskunft, Datenkopie, Berichtigung und Löschung sonstiger Daten). Bei Anfragen von Nutzern, die Sie betreffen, werden wir uns zeitnah mit Ihnen in Verbindung setzen.

Falls wir dies über einen gesonderten Kontakt machen sollen, teilen Sie uns gerne Ihren zuständigen Ansprechpartner mit. Die Datenschutzerklärung werden wir, soweit möglich, im Umfeld der Werbung verlinken, ohne dass von Ihnen dazu eine eigenständige Verlinkung erforderlich ist.

Die Art. 12 ff. DSGVO regeln neue Informationspflichten, die in weiten Teilen über die bisherigen Informationspflichten, die in einer Datenschutzerklärung abzubilden waren, hinausgehen. Falls noch nicht geschehen, muss die Datenschutzerklärung um folgende Punkte ergänzt werden:

- Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters;
- ggf. die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung;
- wenn die Verarbeitung auf Art. 6 Abs. 1 f DSGVO beruht, die berechtigten Interessen, die von den Verantwortlichen oder einem Dritten verfolgt werden;
- ggf. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
- ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln;
- die Dauer der Speicherung der Daten;
- Informationen über das Bestehen eines Rechts auf Auskunft, Berichtigung oder Löschung;
- Information darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist;

- das Vorhandensein von sogenanntem „Profiling“ und in diesen Fällen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Tipp: Prüfen Sie, ob ihre Datenschutzerklärung und ihr Verfahrensverzeichnis alle notwendigen Angaben enthalten, und ergänzen Sie sie gegebenenfalls.

Neue Definition der personenbezogenen Daten

Der Begriff der personenbezogenen Daten wurde in der DSGVO neu definiert. Prüfen Sie daher, welche Auswirkungen das auf Ihr Geschäftsmodell hat. Viele Daten, die früher als anonym galten, sind zukünftig Daten mit Personenbezug. „Personenbezogene Daten“ im Sinne der DSGVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung durch

- eine Kennung wie einem Namen,
- eine Kennnummer,
- Standortdaten,
- eine Online-Kennung oder
- einen oder mehrere besondere Merkmale identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Wichtig für die Onlinebranche ist insoweit ein durch die DSGVO eingeführter Paradigmenwechsel. Während es früher umstritten war, ob Online-Identifier wie Cookie-IDs, User-IDs, MAC-Adressen u. ä. personenbezogene Daten waren, gelten sie nunmehr in der Regel als personenbezogen. Denn es handelt sich hierbei um eine „Online-Kennung" im oben erwähnten Sinne.

Die praktischen Auswirkungen sind erheblich. Denn wenn es sich bei Online-IDs um personenbezogene Daten handelt, dann bedarf jede Erhebung oder Nutzung dieser IDs – etwa im Rahmen von Online-Werbung – der Einwilligung des Nutzers. Deshalb gelangt in diesen Fällen der neue Art. 6 Abs. 1 f DSGVO zur Anwendung (siehe unten 3.), der zukünftig für die Onlinewerbebranche von kaum zu unterschätzender Bedeutung werden dürfte.

Tipp: Prüfen Sie, ob Sie Daten verarbeiten, die früher als anonym galten und in Zukunft als personenbezogen anzusehen sind, denn dann gilt die DSGVO.

Neue Regeln für die Einwilligung von Kindern

Art. 8 DSGVO bestimmt, dass künftig die Einwilligung eines Kindes nur wirksam ist, wenn das Kind das 16. Lebensjahr vollendet hat. Hat das Kind noch nicht das 16. Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern durch die Eltern die Zustimmung erteilt wird.

Tipp: Prüfen Sie, ob Sie Daten von Kindern unter 16 Jahren verarbeiten, denn dafür benötigen Sie die Zustimmung der Eltern.

- Überarbeitung der **technischen und organisatorischen Maßnahmen** (TOMs) und deren Dokumentation. Insbesondere wird eine weitest mögliche Verschlüsselung (SSL o.Ä.), auch bei der Übertragung von Daten zwischen dem Nutzer und unseren Servern (bspw. Cookie-Kennung) und zwischen unseren Servern und denen unserer Partner (bspw. Werbeanfrage), hergestellt. Soweit Sie noch unverschlüsselt an unsere Server angebunden sind, werden wir uns mit Ihnen in Verbindung setzen, um zu prüfen, ob die Anbindung verschlüsselt werden kann. Die Zuordnung eines Nutzers zu Kategorien, die (einzeln oder zusammen) dessen Identifizierung ermöglichen, wird ausgeschlossen. Das gleiche gilt für die nach der DSGVO besonders geschützten Datenkategorien (wie rassische / ethnische Herkunft, politischen Meinungen, religiöse Überzeugungen, genetischen / biometrischen Daten). Soweit die Zuordnung zu den einzelnen Kategorien bei Ihnen vorgenommen wird, sollten Sie diese Vorgaben ebenfalls umsetzen. Der Do-Not-Track-Header wird auch insoweit berücksichtigt, als dass vorhandene Cookies gelöscht und keine Cookies mehr gespeichert werden.

- **Neu: Profiling – und warum Nutzerprofile nicht darunterfallen**

Neu ist in der DSGVO der Begriff des „Profilings". Jede Person sollte nach dem Willen des Gesetzgebers das Recht haben, nicht einer Entscheidung zur Bewertung von ihren persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dies könnte etwa die automatische Ablehnung eines Online-Kreditantrags oder ein Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen sein.

Zu einer derartigen Verarbeitung zählt auch das sogenannte „Profiling". Es meint jegliche Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlichen Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person.

Die gilt allerdings nur, soweit dies rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Im Klartext heißt das, dass jede Form von Nutzerprofilen im Rahmen der Onlinewerbung nicht darunterfallen. Denn diese haben in der Regel keine „rechtlichen Wirkungen".

- Überarbeitung unseres **Verfahrensverzeichnisses**, insbesondere eine laufende Verzeichnisführung mit den neuen TOMs. Dies ist unter anderem erforderlich, um unsere Rechenschaftspflicht nach der DSGVO erfüllen zu können. Zusammen mit den überarbeiteten TOMs wird das Verfahrensverzeichnis unser neues Datenschutzkonzept widerspiegeln und dessen Umsetzung dokumentieren. Bei Bedarf werden wir Ihnen unser Datenschutzkonzept gerne zur Verfügung stellen.

- Überarbeitung der Vereinbarung für die **Auftragsverarbeitung** (bisher: Auftragsdatenverarbeitung; ADV). Insbesondere werden wir die neuen TOMs einbeziehen und die gesetzlichen Einschränkungen der DSGVO auch vertraglich weitergeben. Dies wird unter anderem zu einem Verbot von Profiling im Sinne einer Benachteiligung von Nutzern wegen der Zuordnung zu einer Werbekategorie und zu einem Verbot von Targeting führen, das an Kinder und Jugendliche unter 16 Jahren gerichtet ist. Soweit Sie für uns oder wir für Sie als Auftragsverarbeiter tätig sind, werden wir Ihnen die Vereinbarung natürlich weiterleiten, sobald sie uns vorliegt. Bitte beachten Sie, dass Sie auch unabhängig von uns Maßnahmen zur Erfüllung der DSGVO treffen müssen. Dies dürfte letztlich dazu führen, dass Sie die dargestellten Maßnahmen ohnehin umsetzen werden.

- Datenschutzrechtliche Voreinstellungen, Art. 25 DSGVO

  Neu ist die Verpflichtung für alle Unternehmen, zukünftig datenschutzfreundliche Voreinstellungen vorzunehmen. Es besteht gemäß Art. 25 DSGVO die Pflicht, geeignete technische und organisatorische Maßnahmen vorzunehmen, die sicherstellen, dass durch die Voreinstellung grundsätzlich nur diejenigen personenbezogenen Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, auch

wirklich verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden. ADEX stellt sicher das diese Anforderungen erfüllt werden.

Recht auf Löschung (Recht auf Vergessenwerden), Art. 17 DSGVO

Art. 17 DSGVO hat ein neues Recht, das sogenannte „Recht auf Vergessenwerden" eingeführt. Geblieben sind aber die üblichen Rechte auf Löschung der eigenen personenbezogenen Daten.

Insoweit bestimmt Art. 17 Abs. 1 DSGVO zunächst, dass jeder Betroffene das Recht hat, von dem jeweils Verantwortlichen zu verlangen, dass ihn betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der nachfolgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich.

ADEX bietet die Möglichkeiten Daten von Nutzern gezielt zu löschen

Recht auf Datenübertagbarkeit

Neu ist auch das Recht auf Datenübertragbarkeit, Art. 20 DSGVO. Jede betroffene Person hat danach das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen – zum Beispiel Facebook - bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Ferner hat sie das Recht, diese Daten einem anderen Verantwortlichen (zum Beispiel Google +) ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln.

ADEX bietet die Möglichkeiten Daten gezielt zu exportieren

Haftungserstreckung auf ausländische Unternehmen

Die Haftung nach der DSGVO trifft zukünftig auch ausländische Unternehmen, selbst wenn sie keine eigene Filiale in einem Mitgliedsstaat der Europäischen Union unterhalten. Gemäß Art. 3 DSGVO reicht es aus, dass ausländische Unternehmen entweder betroffenen Personen in der EU Waren oder Dienstleistungen anbieten oder – und das dürfte für die Onlinemarketingbranche wichtig sein – dass diese Unternehmen das Verhalten betroffener Personen „beobachten“, soweit ihr Verhalten in der EU erfolgt. Unternehmen der Onlinemarketingbranche, die also Techniken, insbesondere zur Nachverfolgung von Internetaktivitäten, wie z. B. bei Tracking, Profiling und Targeting einsetzen, haften nach den Bestimmungen der DSGVO selbst dann, wenn sie keine eigene Niederlassung in der EU betreiben.

Tipp: Prüfen Sie, ob Sie mit Unternehmen zusammenarbeiten, auf die dies zutrifft.

- Eine Übermittlung von personenbezogenen Daten in **Drittstaaten** wird nur ausnahmsweise erfolgen. Unsere Datenverarbeitung wird nach wie vor innerhalb der EU stattfinden. Darauf legen wir grundsätzlich auch bei unseren Partnern wert. Soweit einzelne Partner Daten außerhalb der EU verarbeiten, werden wir sicherstellen, dass entweder für den jeweiligen Staat ein Angemessenheitsbeschluss der EU vorliegt, oder dass die Standard-Datenschutzklauseln der EU vereinbart worden sind. Bei Partnern, bei denen eine Auftragsverarbeitung vorliegt, wird letzteres mit der ADV erfolgen.

- Unseren **Datenschutzbeauftragten** werden wir bei der zuständigen Aufsichtsbehörde melden. Dies ist einerseits vorgeschrieben und erleichtert andererseits die Zusammenarbeit. Der Datenschutzbeauftragte wird unsere Mitarbeiter zum neuen Recht schulen (Meldepflichten, Bearbeitung von Betroffenenanfragen, Einbeziehung von Partnern etc.). Außerdem wird er die Überarbeitung der rechtlichen Dokumente begleiten (Datenschutzerklärung, TOMs, Verfahrensverzeichnis und ADVs).

Für die **Onlinebranche** enthält die oben erwähnte erste Voraussetzung eine wichtige Regelung. Denn danach bedarf eine automatisierte Verarbeitung von Daten – die in der Onlinebranche häufig vorkommt – nur dann einer Datenschutz-Folgenabschätzung, wenn diese entweder **Rechtswirkung** gegenüber natürlichen Personen entfaltet oder besonders sensible Daten verarbeitet werden. Die Auslieferung von programmatischer Werbung auf der Basis von möglicherweise erstellten Nutzerprofilen entfaltet aber in der Regel keine Rechtswirkung; in der Regel werden auch keine besonderen Arten personenbezogener Daten verarbeitet. In vielen Fällen der Onlinewerbung wird es deshalb nicht erforderlich sein, eine Datenschutzfolgenabschätzung vorzunehmen.