



Leitfaden zur EU-DSGVO

Datenschutzrechtlichen Anforderungen an kleine und mittelgroße Unternehmen bei Inkrafttreten der Neuen Datenschutzgrundverordnung (DSGVO) am 25. Mai 2018

Illustrator*innen, die auf ihrer Webseite ausschließlich sich selbst mit ihren Illustrationen und Kontaktdaten präsentieren, keine Werbeanalysetools wie z.B. Google-Analytics, kein Kontaktfeld, keine Kommentarfunktionen und keine Newsletter Anforderung installiert haben, verarbeiten keine Daten.

ABER: Sobald Geschäfte online abgewickelt werden, müssen zwangsläufig Daten verarbeitet werden. Soweit es sich hierbei um personenbezogene Daten handelt (auch Email-Adresse eines Kunden) oder Daten gespeichert werden (auch manueller Eintrag ins Adressbuch) stellt die DSGVO neue Anforderungen an den Verwender:

- Jede Datenverarbeitung personenbezogener Daten muss durch die Einwilligung des Betroffenen abgedeckt oder ausdrücklich im Gesetz erlaubt sein.
- Der Umfang der zu verarbeitenden Daten muss dem Zweck angemessen und auf das notwendige Maß beschränkt sein.
- Alle Betroffenen müssen informiert werden, dass und welche Daten in Bezug auf ihre Person erhoben werden. Dabei ist Datenerhebung sowohl das automatische Sammeln über ein Kontaktfeld, als auch das manuelle Sammeln und Eintragen in ein Adressbuch, nachdem ein Kunde eine E-Mail geschickt hat.
- Ab einer Betriebsgröße von 10 Beschäftigten ist ein Datenschutzbeauftragter vorgesehen.

Das erfordert folgende Maßnahmen für Illustrator*innen:

1. Datenerhebung: Einwilligungserklärung

Wer zur Anbahnung oder zur Erfüllung eines Vertragsverhältnisses online mit potenziellen Kunden korrespondiert, benötigt die entsprechenden Angaben der Betroffenen. Die Speicherung dieser zum Abschluss und zur Abwicklung eines Vertrages erforderlichen Daten, wie z.B. Name, Anschrift, Telefonnummer, Kontonummer, bedürfen für die Dauer der Vertragsabwicklung keiner gesonderten Einwilligung des Kunden. Danach sind sie zu löschen.

Erforderlich ist eine Einwilligung für die Verarbeitung darüber hinaus gehender Daten wie Emailadresse, Geburtsdatum, Kaufinteressen und/oder Fotos. Also Daten, die nicht zwingend notwendig für die Erfüllung des Vertrages sind. Auch für den Versand von Werbepost oder Newsletter benötigen Illustrator*innen eine explizite Einwilligung des Adressaten.



Was ist zu tun?

Werden Daten dieser Art über ein Kontaktformular abgefragt sollte eine elektronische Einwilligungserklärung formuliert sein, die der Betroffene – optimaler Weise mit einer kurzen Mail – bestätigen muss. Diese Einwilligungserklärung informiert den Kunden, welche Daten erhoben werden und zu welchem Zweck Sie die jeweiligen Daten verarbeiten wollen. Es darf keine voreingestellte Einwilligung in Form eines Häkchensetzens verwendet werden.

Eine Einwilligungserklärung zur Datenspeicherung und -Verwendung kann auch dem jeweiligen Angebot zum Auftrag beigelegt werden. Die gewährte Einwilligung muss dokumentiert werden, damit im Streitfall der Nachweis hierfür geführt werden kann.

Siehe Dokument

Mustertext Einwilligungserklärung

2. Datenverarbeitung: Datenschutzerklärung

Der Pflichtenkatalog von Illustrator*innen erweitert sich erheblich, wenn die beim Kunden erhobenen personenbezogenen Daten an Dritte weitergegeben oder durch einen externen Dienstleister bearbeitet und/oder gespeichert werden.

Hierunter fallen sowohl die Nutzung externer Serverkapazitäten, als auch die Entsorgung von Datenträgern oder Akten und insbesondere die Nutzung von Google Analytics. In diesen Fällen bleibt die volle Verantwortlichkeit dafür, dass der Datenschutz nicht verletzt wird, beim Illustrator/bei der Illustratorin. Die Daten dürfen nur anhand der konkreten Weisungen des Auftraggebers genutzt werden.

Auf Illustratorenwebsites können beispielsweise folgende Punkte zutreffen:

- Setzen von Cookies
- Newsletter-Abo
- Kontaktformular
- Blog
- Verlinkungen zu Social Media und/oder Like/Share-Buttons
- Analyse-Tools (z.B. Adobe Analytics, Google Analytics, u.a.)
- Google Maps
- Google Fonts
- WordPress-Plug-ins
- Allgemeine Daten, die der Provider der Webseite von jedem Webseitenbesucher erfasst (Logfiles)



Auch kleinere Webseiten verwenden meistens standardmäßig Cookies, um die Nutzerprofile zu analysieren. Wer sich nicht im Klaren darüber ist, welche Tools seine Webseite verwendet, muss dies auf jeden Fall klären. Der Betroffene muss informiert werden, was mit seinen Daten geschieht. Es muss daher in der Datenschutzerklärung genau mitgeteilt werden, inwieweit Cookies gesetzt werden. Im Übrigen muss sofort bei Aufruf der Website ein Hinweis über die Verwendung von Cookies informieren, sei es als Pop-Up-Fenster oder als Fußleiste.

Bezüglich der Tracking- und Analyse Tools muss eine Klausel in der Datenschutzerklärung enthalten sein, die für jedes Tool gesondert dessen Funktionsweise erläutert. Die Besucher-ID muss automatisch anonymisiert werden. Dies gilt insbesondere beim Einsatz von Google Analytics. Auch beim Setzen von sogenannten „LIKE“-Buttons ist zu beachten, dass der Betroffene informiert werden muss, in welche Datennutzung er damit genau einwilligt.

Was ist zu tun?

Auf jeden zutreffenden Punkt muss in der Datenschutzerklärung der Webseite hingewiesen werden und erklärt werden, wie und warum hiermit welche Daten erhoben werden. Hierfür gibt es online Datenschutzerklärungs-Generatoren. Hierbei muss man sich allerdings bewusst sein, dass so eine Instant-Datenschutzerklärung aus einem Online-Tool möglicherweise nicht jede einzelne Funktion der eigenen Webseite abdeckt, und keine Garantie für deren Rechtssicherheit übernommen wird. Welcher Bedarf besteht kann anhand unserer Checkliste für Website geprüft werden.

Siehe Dokument

Mustertext Datenschutzerklärung

Checkliste Website

3. Datenweitergabe: Vereinbarungsvertrag mit Dritten

Beachtet werden muss auch, ob eine Webdesign-Agentur Zugriff auf die personenbezogenen Daten haben kann, die gespeichert sind. Oder auch, ob bspw. der Programmierer Zugang auf die Logfiles nehmen kann. Falls ja, muss der Illustrator auch hier eine Vereinbarung über die Auftragsverarbeitung schließen.

Zusammengefasst: Mit jedem Dritten, an den die personenbezogenen Daten eines Kunden weitergegeben werden, muss eine Vereinbarung über die Verarbeitung der Daten geschlossen werden.

Solche Dritte können beispielsweise sein:

- Webhoster, auf dessen Server man seine Webseite hat
- Agentur oder Administrator der eigenen Webseite



- Newsletter-Anbieter
- Etsy und ähnliche Shop-Anbieter
- Google (beim Einsatz von Google Analytics)
- Cloud-Anbieter (Backups, Dropbox o.Ä.)
- Plug-ins (z.B. für Kontaktformular)

Was ist zu tun?

Diesen Verarbeitungsvertrag (engl.: data Processing Agreement) vom jeweiligen Anbieter anfordern. Diese Unternehmen stellen solche Verarbeitungsverträge selbst zur Verfügung oder stellen sie auf Anfrage. Man muss also selbst keinen Vertrag aufsetzen lassen!

4. Datendokumentation: Verarbeitungsverzeichnis

Jede Verarbeitung personenbezogener Daten muss in einem Verzeichnis dokumentiert werden. Darunter fallen sowohl die oben aufgelisteten Funktionen der Webseite, als auch die ebenfalls genannten Möglichkeiten zur Weitergabe der Daten. Zusätzlich fallen darunter auch die eigene Kundenkartei (ob elektronisch oder auf Papier) sowie Verträge, Rechnungen etc. die Kundendaten enthalten.

Was ist zu tun?

Für jede einzelne dieser Verarbeitungen legt man am eine eigene Tabelle an. Das ist das Verarbeitungsverzeichnis. Darin sollte stehen:

- Name und Kontaktdaten des Verantwortlichen bzw. seines Vertreters
- Der Zweck der Verarbeitung
- Die Rechtsgrundlage, auf der die Verarbeitung erfolgt
- Die Kategorie der betroffenen Personen und personenbezogenen Daten
- Die Kategorie von Empfängern der Daten
- Mögliche Übermittlung in Drittstaaten
- Die Lösungsfrist
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zu Datensicherung

Für den Fall, dass eigene Mitarbeiter*innen eingesetzt werden, müssen diese ebenfalls auf die Vertraulichkeit von Daten verpflichtet und auf den Datenschutz hingewiesen, erforderlichenfalls angemessen geschult werden. Auch diese Hinweise und Verpflichtungen müssen dokumentiert werden.

Man sollte weiter darauf vorbereitet sein, wie man reagiert, wenn ein Betroffener erfahren möchte, welche Daten über ihn gespeichert worden sind. Die Personen, deren Daten gespeichert werden, haben ein Anrecht darauf, zu wissen und zu erfahren, zu welchem Zweck die sie betreffenden, persönlichen Daten gespeichert und ggf. verarbeitet werden.



Dieser Auskunftsanspruch umfasst die Länge der Speicherung, die Empfänger der Daten sowie Art und Folgen der Verarbeitung. Darüber hinaus kann jederzeit die Berichtigung unrichtiger Daten oder die Vervollständigung unvollständiger Daten verlangt werden. Die Betroffenen haben weiterhin einen Anspruch darauf, dass ihre Daten nach entsprechender vereinbarungsgemäßer Nutzung gelöscht werden.

Weiterhin besteht ein Widerspruchsrecht gegen die weitere Datenverarbeitung.

Die geforderten Auskünfte sind unentgeltlich und unverzüglich nach Aufforderung durch den Betroffenen (spätestens innerhalb eines Monats) zu erteilen.

Der Illustrator muss weiterhin ein sogenanntes Lösungskonzept vorsehen, das darlegt, dass und wie nach entsprechender Aufforderung die gespeicherten Daten gelöscht werden. Die personenbezogenen Daten – sofern sie nicht in Geschäftsbriefen oder steuerrelevanten Unterlagen enthalten sind – müssen gelöscht bzw. vernichtet werden, wenn sie nicht mehr benötigt werden.

Siehe Dokument

Vorlage Verarbeitungsverzeichnis

5. Technische Maßnahmen zum Datenschutz: Dokumentation

Alle Funktionen müssen auch auf ihre jeweilige Rechtssicherheit geprüft werden! Die hierzu ergriffenen technischen und organisatorischen Maßnahmen zum Schutz der Daten müssen dokumentiert werden. So ist z.B. eine Übermittlung von personenbezogenen Daten an Dritte per Email ohne weitere Sicherungsmaßnahmen ist datenschutzrechtlich nicht zulässig.

Was ist zu tun?

Einzuhalten sind folgende Schutzvorkehrungen:

- Zutrittskontrolle: es muss sichergestellt werden, dass Unbefugte keinen Zugriff auf die Daten bzw. auf die Datenverarbeitungsanlage haben. Hierzu gehört auch, dass die entsprechenden Räume verschlossen sind. Es muss weiterhin gewährleistet werden, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen Personenbezogene Daten dürfen nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
- Es muss weiter gewährleistet werden, dass die zu unterschiedlichen Zwecken erhobenen Daten (Vertragsabwicklung, Newsletter, Infomails) auch separat verarbeitet werden können, z.B. getrennter Zugriff bei Weitergabe an Dritte.
- Weitergabekontrolle: Es muss sichergestellt werden, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transportes oder bei ihrer Speicherung auf



Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Es muss sichergestellt werden, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystem eingegeben, verändert oder entfernt worden sind.
- Es muss sichergestellt werden, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten in einer Weise dokumentiert werden, dass sie in zumutbarer Weise nachvollzogen werden können.
- Es muss sichergestellt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
- Verfügbarkeitskontrolle: Es muss sichergestellt werden, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Weiterhin wird gefordert, dass Daten so gesichert werden, dass sie bei einem eventuellen Verlust wiederhergestellt werden und dass technische Systeme trotz Störungen oder Teilausfällen aufrechterhalten werden können.

Siehe Dokument

Vorlage TOM