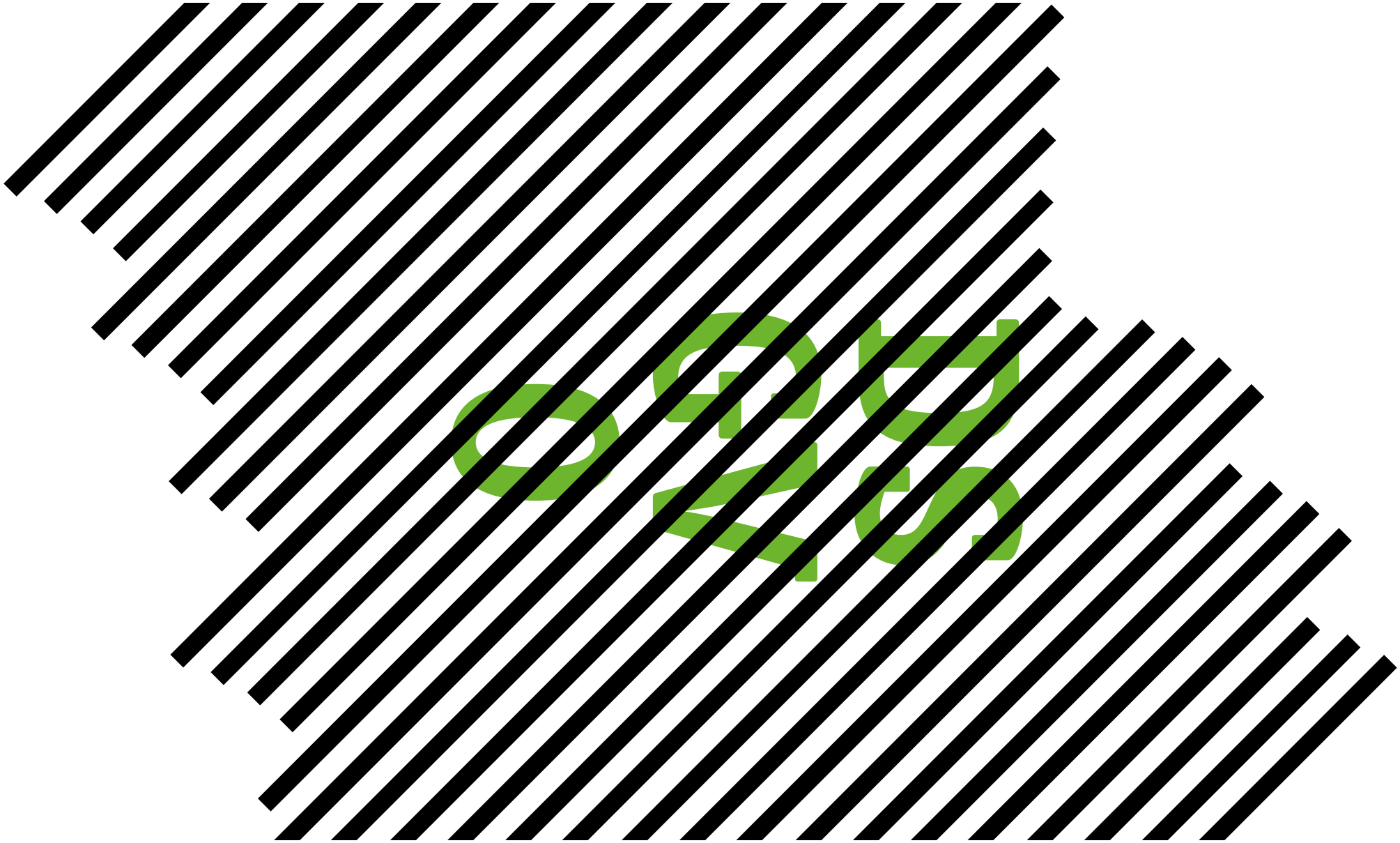
DSGVO im Marketing

Mit der neuen Datenschutzgrundverordnung sollen europaweit personenbezogene Daten besser geschützt werden.
Stichtag ist der 25. Mai 2018. Für viele Unternehmen stellt das eine große Herausforderung dar, denn die neue Verordnung ist komplex und wird vermutlich streng kontrolliert.
Mit diesem Datenschutz-Kit möchten wir Ihnen einen Überblick über die wichtigsten Anforderungen im On- und Offlinemarketing geben.

Folgende Inhalte helfen Ihnen, die nötigen Maßnahmen zu treffen:
– Zusammenfassung: Das müssen Sie wissen
– Checkliste
– Nützliches und Musterverträge

Für Fragen rund um Marketing und Werbung sind wir für Sie da.
Suchen Sie rechtsverbindliche Beratung, vermitteln wir Ihnen gerne Kontakte zu Juristen mit Schwerpunkt Datenschutz.


DSGVO

Grundlagen der DSGVO

HINWEIS: *Dieser Artikel stellt lediglich Anregungen und Hinweise vor und ersetzt auf keinen Fall eine rechtliche Beratung, welche nur Ihr Anwalt beziehungsweise Datenschutzbeauftragter des Vertrauens leisten darf.*

Am 25. Mai 2018 tritt die neue DSGVO in Kraft. Sie reformiert das Datenschutzrecht in nahezu allen Bereichen, zum Teil sind die neuen Vorgaben relativ einfach umzusetzen, zum Teil sind sie jedoch auch sehr komplex. Auf jeden Fall ist es notwendig, dass sich Unternehmer und Betreiber von Webseiten mit den umfassenden Neuregelungen des Datenschutzrechts vertraut machen.

Die DSGVO

Über die DSGVO wird ab dem 25. Mai dieses Jahres der Umgang von Unternehmen mit personenbezogenen Daten europaweit einheitlich geregelt. Zahlreiche der im deutschen Bundesdatenschutzgesetz (BDSG) festgelegten Vorschriften sind dann nicht mehr gültig. Gleichzeitig wird das BDSG neu gefasst.

Ziel der Maßnahme ist es, das Datenschutzrecht innerhalb der EU anzugleichen, so dass Unternehmen sich künftig auf ein europaweit weitestgehend einheitliches Datenschutzrecht verlassen können.

Unternehmen, die ihren Sitz außerhalb der EU haben, sind ebenfalls an die neue DSGVO gebunden, wenn sie Daten von Personen aus der EU verarbeiten. Das bedeutet, dass sich auch soziale Netzwerke und internationale Cloud-Dienste an diese Regeln halten müssen. Denn die DSGVO betrifft ausnahmslos jedes im Internet tätige Unternehmen: Die Vorschriften für Nutzer- Tracking, Kundendaten, Newsletter oder Werbemails, Werbung auf Facebook, die eigene Datenschutzerklärung ändern sich.

Neue Datenschutzerklärung und Impressum

Jede Webseite benötigt grundsätzlich eine neue Datenschutzerklärung nach den Vorgaben der DSGVO. Dabei gelten folgende Grundsätze:

- Eine klare und verständliche Sprache
- Eine vorgeschaltete zusammenfassende Erklärung
- Die Kontaktdaten des Seitenbetreibers
- Nennung des Datenschutzbeauftragten, falls es ihn gibt.
- Die Rechtsgrundlage der jeweiligen Erhebung und Verarbeitung von Daten muss benannt werden (entweder als Einwilligung oder gesetzliche Regelung).

Weiterhin sind in einer Datenschutzerklärung nach DSGVO notwendig:

- Nennung aller Datenverarbeitungsvorgänge auf der Webseite
- Umgang Kunden- / Bestelldaten
- Tracking, Cookies, Social Media
- Newsletter, A(D)V
- Dauer der Speicherung, Löschungsfristen
- Auskunft, Berichtigung, Löschung, Widerspruch
- Recht auf Datenherausgabe und Übertragbarkeit

Eine Einwilligung innerhalb der Datenschutzerklärung ist unzulässig.

Nach Artikel 17 der DSGVO besteht Löschpflicht der Daten wenn:

- der Zweck der Erhebung nicht mehr besteht.
- die Einwilligung widerrufen wurde (zum Beispiel bei der Abmeldung eines Newsletters)
- ein Widerspruch des Nutzers erfolgt, weil er seine Daten gelöscht sehen möchte und keine gesetzlichen Speicherpflichten entgegenstehen (Steuern und Buchhaltung)

Beim Impressum sind derzeit keine Änderungen notwendig.
(Diskutiert wird allerdings, dass für Auskunfts-, Berichtigungs- und Löschungsansprüche ein spezielles Kontaktformular innerhalb der allgemeinen Menüstruktur geschaffen werden soll.

Verarbeitungsverzeichnis

Unternehmen mit mehr als 250 Mitarbeitern und besonderen Datenkategorien benötigen ein Verarbeitungsverzeichnis. Dazu sind auch Unternehmen mit weniger Mitarbeitern verpflichtet, wenn die Verarbeitung nicht nur gelegentlich erfolgt. Eine präzisere Fassung dieser Bestimmung wird noch erarbeitet. Bis dahin sollte im Zweifelsfall ein solches Verzeichnis angelegt werden.

Verarbeitungsverzeichnis - Inhalte

- Angaben des Verantwortlichen
- Name und Kontaktdaten des Verantwortlichen, seines Vertreters und des Datenschutzbeauftragten
- Zwecke der Verarbeitung
- Kategorien betroffener Personen und personenbezogener Daten
- Kategorien von Empfängern
- Übermittlungen von personenbezogenen Daten an ein Drittland
- Löschungsfristen
- Beschreibung der technischen und organisatorischen Maßnahmen
- Angaben des Auftragsverarbeiters
- Name und Kontaktdaten des Auftragverarbeiters und des Verantwortlichen, ihrer Vertreter und des Datenschutzbeauftragten
- Kategorien von Verarbeitungen
- Übermittlungen von personenbezogenen Daten an ein Drittland

Cookies und Tracking

Bei Cookies und Tracking gibt es keine Änderungen. Allerdings werden Cookies spezifisch durch die ePrivacy-Verordnung (ePV) neu geregelt (Vermutlich jedoch erst ab 2019).
Google Analytics bleibt weiterhin wie bisher erlaubt, wenn die folgenden Voraussetzungen erfüllt sind:

- A(D)V Vertrag mit Google abgeschlossen (ist online direkt in der Verwaltung von Google Analytics möglich)
- IP Anonymisierung aktiviert
- Opt-out Möglichkeiten für Desktop und Mobil

Newsletter und Einwilligungen

Einwilligungen von Nutzern, z.B. zum Newsletter-Versand, die bereits nach altem Recht wirksam eingeholt wurden (double opt-in) gelten grundsätzlich weiter.
Ausnahmen: Koppelungsverbot bei alten Einwilligungen nicht beachtet; Einwilligungen durch Minderjährige;

Neuregelung von Newsletter-Aktionen

Wenn keine gesetzliche Erlaubnis zum Speichern oder Übertragen von Daten vorhanden ist, wird immer eine Einwilligung benötigt.
Auch unter der DSGVO sollte das double opt-in Prinzip beachtet werden, um die Einwilligung im Zweifel nachweisen zu können. Wichtig:
Diese Einwilligung muss in jedem Fall elektronisch dokumentiert werden.

Die Einwilligung muss dabei „freiwillig“ erfolgen: Echtes Koppelungsverbot in Art. 7 Abs.4 DSGVO.
In der Regel: Keine Daten gegen Inhalte (z.B. E-Books, Gewinnspiele, Checklisten) und keine Koppelung von Newsletter-Versand an Vertragsschluss.

Wirksamkeit von älteren Einwilligungen
Wenn Kunden weiterhin per Post oder Mail mit Werbung erreicht werden sollen, sind grundsätzlich Einwilligungen, die wirksam nach altem Recht eingeholt wurden, auch nach der DSGVO gültig. Ausnahmen nach der neuen DSGVO: Wenn beispielsweise die Einwilligung nicht freiwillig erteilt wurde, weil sie an ein anderes Angebot gekoppelt war, gilt sie nicht weiter. Darüber hinaus gilt eine Einwilligung nicht, wenn sie von einem Minderjährigen unter 16 Jahren ohne elterliche Einwilligung erteilt wurde.

Kundendatei und schriftliche Erklärungen
Mündlich erteilte Einwilligungen lassen sich im Ernstfall kaum nachweisen. Einwilligungen sollten deshalb stets schriftlich oder elektronisch eingeholt werden.

Bestandskunden und Werbung per E-Mail
Unter bestimmten Voraussetzungen können Unternehmen Bestandskunden auch ohne Einwilligung und auch zu ähnlichen Angeboten werblich kontaktieren. Dafür gelten die folgenden Voraussetzungen:

- E-Mail-Adresse im Zusammenhang mit einem wirksamen Vertrag (bloße Anfragen oder widerrufener Vertrag genügen nicht)
- Werbung für ähnliche Leistungen oder Waren
- kein Widerspruch des Kunden
- Hinweis auf Austragung bei Erhebung und jeder Verwendung der E-Mail-Adresse (Registrierung)

Empfohlen wird, dass bei der Registrierung von Kunden bzw. bei der Bestellung ein Hinweis darauf enthalten ist, dass der Empfänger der Nutzung seiner E-Mail-Adresse jederzeit widersprechen kann.
Wenn es sich nicht um Bestandskunden handelt, ist der Kunde umfassend über die beabsichtigte Werbung zu informieren.

Datenschutzbeauftragter

Ein Datenschutzbeauftragter ist zu benennen von Unternehmen, die in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen oder zu einer Datenschutz-Folgeabschätzung nach Artikel 35 DSGVO verpflichtet sind (Einzelheiten unten bei Ziff. 9.).

Interessenskonflikte
Ein Vorstandsmitglied, Geschäftsführer oder der Unternehmensinhaber kann nicht gleichzeitig auch Datenschutzbeauftragter sein, weil dadurch ein Interessenkonflikt zwischen dem Unternehmen und den datenschutzrechtlichen Vorschriften entstehen könnte. Um Konflikte zu vermeiden, kann ein externer Datenschutzbeauftragter bestellt werden.

Qualifikationen des Datenschutzbeauftragten
Der Datenschutzbeauftragte muss zuverlässig sein und über juristische Kenntnisse und technische Sachkunde verfügen. Um die notwendigen Qualifikationen zu vermitteln, werden Schulungen und Seminare inkl. Prüfung bundesweit angeboten (u. a. beim TÜV).

Mitarbeiterdaten

Die DSGVO enthält zahlreiche Pflichten und Obliegenheiten, die der Arbeitgeber im Sinne des Mitarbeiterschutzes künftig einhalten muss.

Mitarbeiterdaten sollen nur dann verarbeitet werden, wenn dies für die Entscheidung über die Einstellung eines Bewerbers oder zur Durchführung, Ausübung oder Beendigung eines Arbeitsverhältnisses erforderlich ist. Erlaubt ist die Verarbeitung auch dann, wenn sie für die Erfüllung gesetzlicher Rechte und Pflichten, eines Tarifvertrags oder einer Betriebs- oder Dienstvereinbarung oder im Falle einer Strafverfolgung erforderlich ist. Ob die Erhebung bestimmter Daten erforderlich ist, wird dabei grundsätzlich anhand des konkreten Einzelfalls bestimmt.
Wer rechtlichen Unsicherheiten rund um die „Erforderlichkeit" aus dem Wege gehen will, kann freiwillig abgegebene Einwilligungen von seinen Arbeitnehmern einholen. Im Streitfall muss eine behauptete Freiwilligkeit der Einwilligung vom Arbeitgeber allerdings nachgewiesen werden.
Für eine wirksame Einwilligung gelten bestimmte formale Kriterien.
Sie muss grundsätzlich in Schriftform erfolgen und eigenständig unterschrieben sein. Da das nicht immer praktikabel ist, kann unter besonderen Umständen auch eine elektronische Einwilligung eingeholt werden.
Zudem muss der Beschäftigte in geeigneter Form darauf hingewiesen werden, dass die Einwilligung jederzeit widerrufbar ist. Bestimmte Voraussetzungen für die Widerrufserklärung müssen dabei vom Arbeitgeber geschaffen werden.
Ein Arbeitgeber muss die Einhaltung der hier genannten Pflichten im Zweifel nachweisen können (Dokumentationspflichten). Überdies sind Arbeitgeber nach der DSGVO mit strengeren Informationspflichten bei Datenschutzverstößen und zahlreichen weiteren Pflichten (u. a. Löschungspflichten) konfrontiert.

Im Hinblick auf diese Pflichten ist es empfehlenswert, dass Arbeitgeber ihre unternehmensinternen Prozesse überprüfen und gegebenenfalls anpassen. (Compliance-Management).

Auftrags(daten)verarbeitung

Wird die Erhebung und Verarbeitung personenbezogener Daten durch ein externes Unternehmen vorgenommen, muss dies nach wie vor vertraglich geregelt werden. Zum Beispiel wenn eine Agentur Werbemaßnahmen ausführt, bei einem externen Newsletter-Anbieter, Webhoster, externen Wartungsverträgen.

A(D)V-Verträge

Hier gibt es nur wenige inhaltliche Neuregelungen. Dazu zählen:

- Der Auftragsverarbeiter muss unter Umständen ein Verfahrensverzeichnis führen, die Weisungen des Verantwortlichen protokollieren.
- Die Schriftform ist bei Verträgen nicht mehr notwendig.

Joint-Controllership Vereinbarung

Wenn die Daten von mehreren Unternehmen in gemeinsamer Verantwortung verarbeitet werden, muss eine Joint-Controllership Vereinbarung geschlossen werden, in der die einzelnen Zuständigkeitsbereiche festgelegt werden müssen.

Datenschutz bei Minderjährigen

Bei Jugendlichen unter 16 Jahren müssen die Eltern einwilligen. Allerdings gilt dies lediglich für Fälle, bei denen die DSGVO eine Einwilligung vorschreibt (z.B. für Werbung) und in der Praxis nur dann, wenn es sich um Angebote handelt, die sich direkt an Kinder und Jugendliche richten.
Bei gemischten Angeboten für Erwachsene und Jugendliche sind keine spezifischen Vorgaben festgelegt.

Datenschutz-Folgenabschätzung

In bestimmten Fällen sind Sie verpflichtet, die Folgen der Datenverarbeitung zu bewerten und dies in einer Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO festzuhalten. Eine sog. DSFA ist immer dann durchzuführen, wenn „eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten zur Folge hat“. Dies ist unter anderem der Fall bei der Verarbeitung von Gesundheitsdaten, Religion, Sexualität. Bei Geschäftsgeheimnissen, Profiling/Scoring, strafbaren Handlungen.

Einsichtsrecht und Meldepflicht

Nach Artikel 15 der DSGVO haben Betroffene das Recht, über ihre gespeicherten personenbezogenen Daten informiert zu werden. Die Auskunft darüber kann in schriftlicher Form als Brief oder E-Mail oder auch mündlich erfolgen und zwar unverzüglich, jedoch spätestens einen Monat nach Eingang des Antrags.

Datenpannen

Bei Datenpannen gelten strengere Anforderungen als bisher. Sie sollten gegenüber Aufsichtsbehörden unverzüglich, nach Möglichkeit innerhalb 72 Stunden, gemeinsam mit einer umfassenden Dokumentation vorgelegt werden (Art 33 DSGVO).

Inhaltliche Details sind nach Art. 33 Abs. 5 DSGVO geregelt:
https://dejure.org/gesetze/DSGVO/33.html

Bußgelder und Abmahnungen

Bei Verstößen gegen das Datenschutzrecht drohen Abmahnungen und Gerichtsverfahren, denn das Datenschutzrecht hat wettbewerbsrechtliche Relevanz. Verstöße können auch nach der DSGVO abgemahnt werden.

Bis zu 20 Millionen Euro Bußgeld

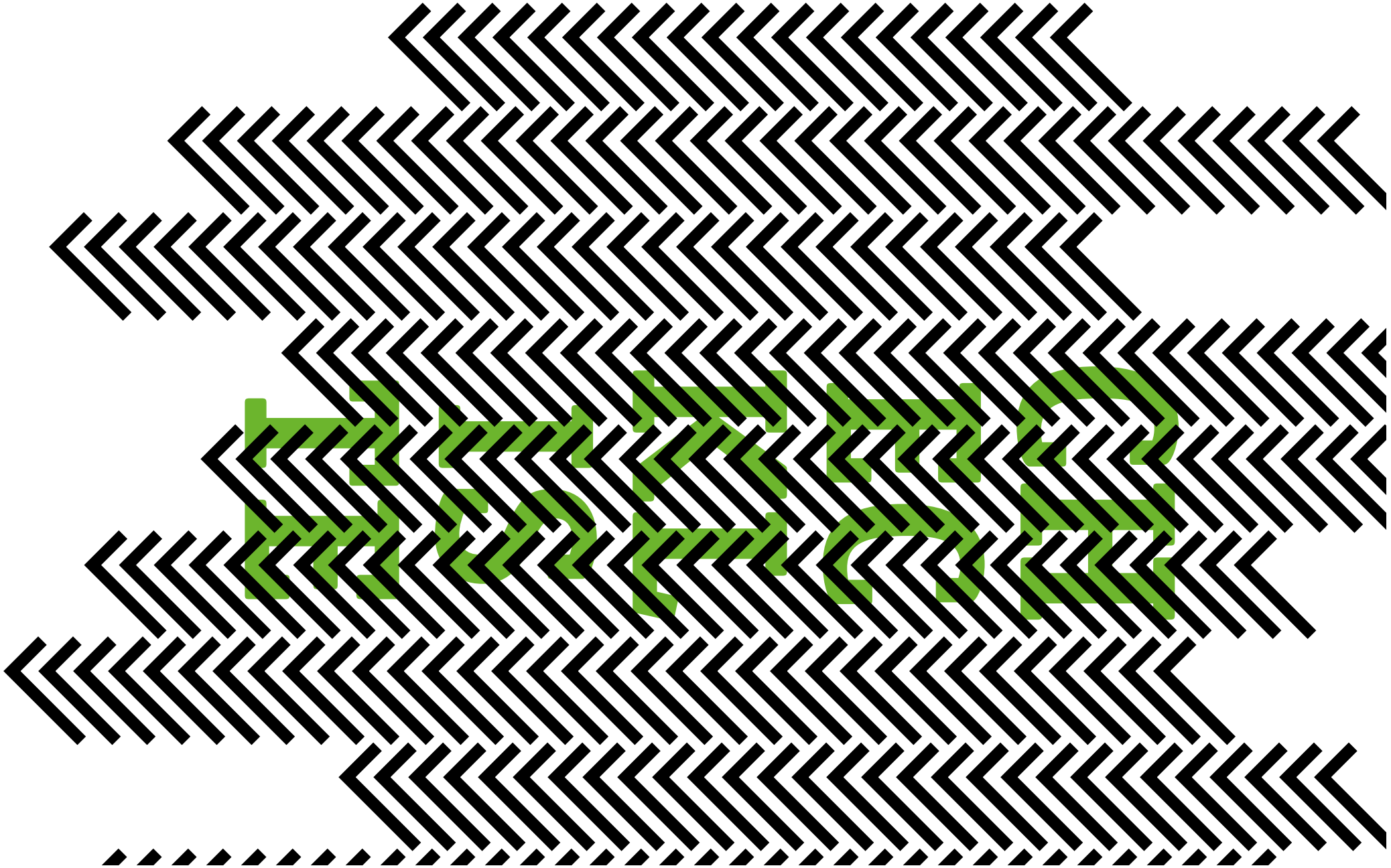
Ein Kernbestandteil der neuen DSGVO ist der neu gefasste Bußgeldrahmen mit bis zu 20 Millionen Euro oder 4% des weltweiten Umsatzes aus dem Vorjahr. Dabei wird sich die Festlegung der Bußgelder gegenüber der bisherigen Praxis verschärfen, d. h. die Höhe der Bußgelder wird aller Voraussicht nach steigen.
Wichtig ist es deshalb, die Anfragen bzw. Beschwerden von Nutzern und von Datenschutzbehörden unbedingt ernst zu nehmen und möglichst umgehend auf sie zu reagieren.

Maßnahmen zum Schutz der Daten

Ein zentraler Punkt ist, dass Kundendaten nach dem Datenschutzrecht korrekt und für den Endverbraucher sicher abrufbar gespeichert werden. Dabei hängt die Auswahl der geeigneten technischen und organisatorischen Maßnahmen vom Risiko der Datenverarbeitung ab. Je sensibler die Daten sind, desto intensivere Sicherungsmaßnahmen sind erforderlich. Wichtig ist dabei, dass die Maßnahmen dem Stand der Technik entsprechen. Zwar macht die DSGVO hier keine konkreten technischen Vorgaben, fordert jedoch angemessene technische und organisatorische Maßnahmen zum Schutz der Daten.

Zur Orientierung folgt hier eine Auflistung möglicher Maßnahmen, wie sie in § 64 des neuen Bundesdatenschutzgesetzes formuliert sind.

- **Zugangskontrolle:** Verwehrung des Zugangs zu Verarbeitungsanlagen für Unbefugte.
- **Datenträgerkontrolle:** Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern.
- **Speicherkontrolle:** Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten.
- **Benutzerkontrolle:** Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte.
- **Zugriffskontrolle:** Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.
- **Übertragungskontrolle:** Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können.
- **Eingabekontrolle:** Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind.
- **Transportkontrolle:** Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden.
- **Wiederherstellbarkeit:** Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.
- **Zuverlässigkeit:** Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden.
- **Datenintegrität:** Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können.
- **Auftragskontrolle:** Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.
- **Verfügbarkeitskontrolle:** Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.
- **Trennbarkeit:** Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.


Checkliste

Ist Ihr Internetauftritt DSGVO-Ready?

Haben Sie ein Impressum?
Wenn ja: Ist es aktuell und erfüllt alle Anforderungen?
Stichwort: USt-ID Nr., Online-Streitschlichtung, Rechtsform, Ansprechpartner, ...

Haben Sie eine Datenschutzerklärung?
Wenn ja: Entspricht sie bereits den DSGVO-Anforderungen
und ist auf den ersten Blick erreichbar?

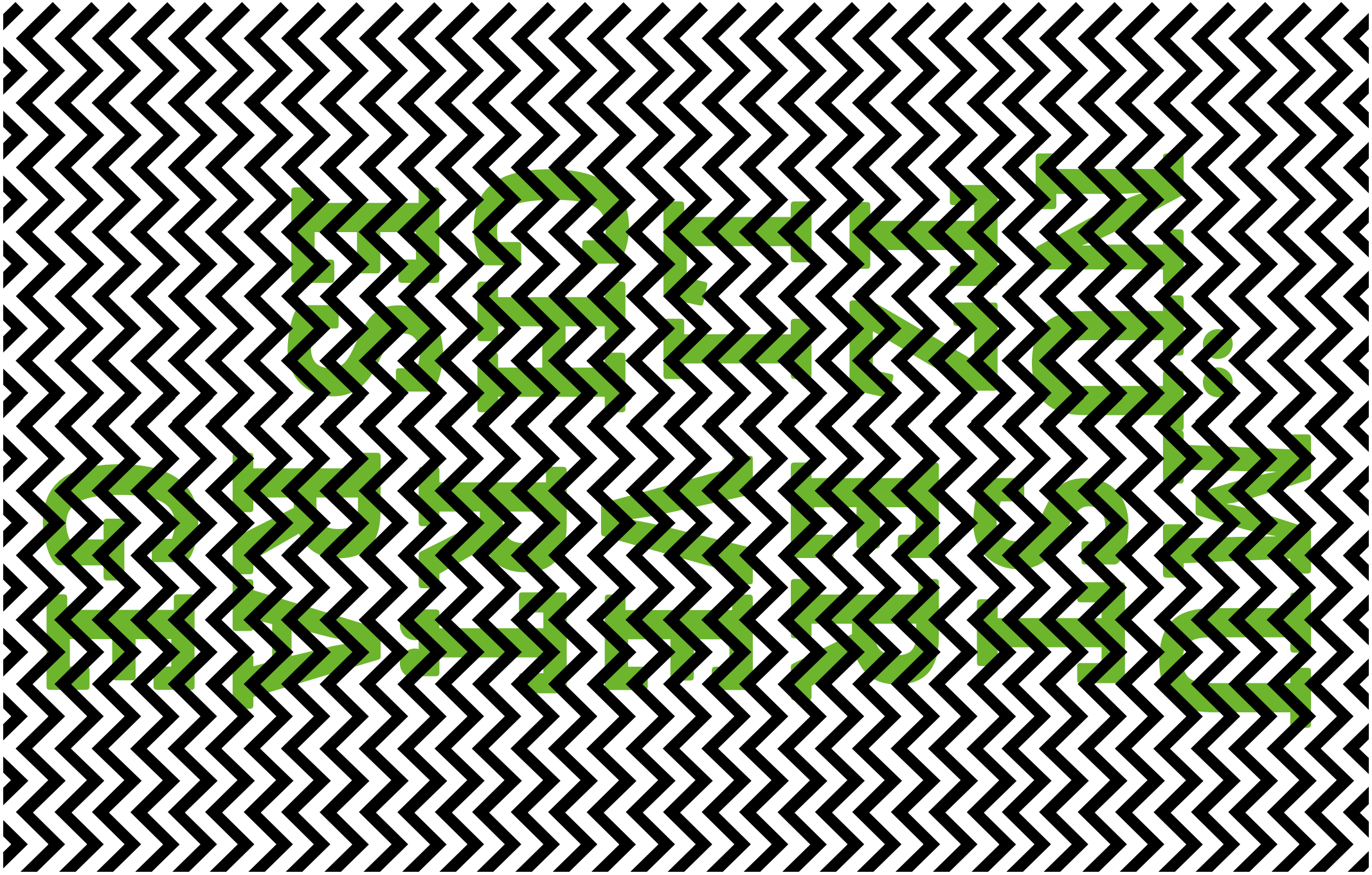
Verfügt Ihr Auftritt bereits über ein Sicherheitszertifikat
bzw. ist er über https erreichbar?
Oder: Sehen Sie ein kleines grünes Schloss oben in der Adresszeile?

Haben Sie ein Kontaktformular?
Wenn ja, gibt es Felder (z. B. Straße, Wohnort) die man weglassen könnte,
ohne dass die Anfrage sinnlos wird? Stichwort: Datensparsamkeit.

Sind in Ihrem Auftritt sogenannte Social Plugins eingebunden
(z. B. Share-Buttons von Facebook, Twitter o. ä.)?
Wenn ja, sind diese konform eingebunden?

Kommen im Hintergrund Cookies zum Einsatz?

Haben Sie ein Statistiktool eingebunden wie z. B. Google Analytics
oder Piwik/Matomo?
Wenn ja, sind diese Tools bereits nach den neuesten Anforderungen eingebunden?
Stichwort: Opt-Out Cookies, IP-Anonymisierung.



Nützliches & Musterverträge

Nützliches & Musterverträge

10-Punkte-Checkliste der Datenaufsichtsbehörden
https://www.hannover.ihk.de/fileadmin/data/Dokumente/Themen/Recht/10-Punkte-Papier_PM_Datenschutz_bleibt_Chefsache.pdf

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
https://www.bvdnet.de/datenschutzbeauftragten-finden/

Fragebogen zur Umsetzung der DS-GVO
https://www.hannover.ihk.de/fileadmin/data/Dokumente/Themen/Recht/Newsletter_Nr._7_BayLDA-DSGVO-Fragebogen_endg-1.pdf

Mustervertrag zur Auftragsdatenverarbeitung
https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/EU-DSG/170515-Auftragsverarbeitung-Anlage-Mustervertrag-online.pdf

Mustereinwilligung in die Nutzung von Mitarbeiterfotos
https://www.activemind.de/datenschutz/dokumente/einwilligung-mitarbeiterfotos/

Bahnhofstraße 46
27305 Bruchhausen-Vilsen
Fon 04252.93868-0
E-Mail: dh@diersundhemmje.de
www.diersundhemmje.de

DIERS+HEMMJE
KREATIVE KOMMUNIKATION