REP
WIRTSCHAFTSPRÜFUNGS-GMBH
Krugerstraße 6
1010 Wien

Betroffene: Unternehmen und Datenschutzbeauftragte

Diese Regeln sind für alle Unternehmen relevant, die Mitarbeiter beschäftigen. Insofern sind zahlreiche Firmen doppelt betroffen: Hinsichtlich des Datenschutzes ihrer Angestellten (Beschäftigungsdatenschutz) und in Bezug auf Kunden, Lieferanten und Webseitenbesucher.

Eine besondere Relevanz hat die DSGVO natürlich für die Berufsgruppe der **Datenschutzbeauftragten**. Ihre Zahl wird durch die DSGVO europaweit beträchtlich wachsen. Denn künftig müssen europaweit alle öffentlichen Stellen und **alle Unternehmen, deren Kerntätigkeit sich auf die Handhabung von Personendaten bezieht**, einen betrieblichen Datenschutzbeauftragten benennen. Selbst wenn die Kerntätigkeit nicht auf die Datenverarbeitung bezogen ist, muss ein Datenschutzbeauftragter bestellt werden, wenn im Betrieb mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Das dürfte für zahlreiche Mittelständler gelten. Spätestens bis Mai 2018 muss bei Unternehmen, die von dieser Regelung betroffen sind, eine Benennung erfolgt sein. Doch auch für andere Unternehmen kann es sinnvoll sein, kurzfristig einen Datenschutzbeauftragten einzustellen, um den Übergangsprozess zur EU-Datenschutz-Grundverordnung im Mai 2018 rechtssicher zu gestalten.

Auch für **Datenschutzbeauftragte**, die bereits in einem Unternehmen angestellt sind, bedeutet die Datenschutz-Grundverordnung eine große Umstellung. Denn ihre Rolle im Unternehmen ändert sich grundlegend: Sollte der Datenschutzbeauftragte bisher auf die Datenschutz-Konformität *hinwirken*, so ist er künftig für die *Überwachung* der Maßnahmen verantwortlich. Damit weitet sich sein Aufgabenfeld aus und auch **sein Haftungspotenzial steigt**.

Für Datenschutzbeauftragte bedeutet die neue Verordnung also eine Menge Arbeit: Sie müssen sich detailliert in die neue Gesetzeslage einarbeiten. Dennoch hat das neue Gesetz für sie auch positive Seiten: **Ihre Expertise wird in nächster Zeit besonders gefragt** sein und mit den zunehmenden Aufgaben ist auch eine Aufwertung ihrer Position im Unternehmen verbunden.
Im Folgenden geben wir eine Zusammenfassung der Datenschutz-Grundverordnung, die besonders die Neuerungen für Webseitenbetreiber und Unternehmen berücksichtigt.

Auswirkungen: Unternehmen aufgepasst

Auch, wenn es keine grundlegende Neuausrichtung des Datenschutzes gibt, **bringt die europäische Datenschutz-Grundverordnung im Detail viele Veränderungen**. Diese müssen Unternehmen unbedingt berücksichtigen und bereits bei der Konzeption von Arbeitsabläufen mit Personenbezug in ihren Workflow integrieren (Prinzip des *Privacy by Design*). Andernfalls verstoßen sie gegen europäisches Recht. Es folgen die wichtigsten Neuregelungen, die Unternehmen – insbesondere im Bereich des Onlinehandels – beachten müssen.

Allgemeine Datensicherheit in Unternehmen

- **Datenschutz-Folgeabschätzung (DSFA)**: Unternehmen sind verpflichtet, Risiko-Abschätzungen vorzunehmen. Sie müssen außerdem festhalten, welche Schutzmaßnahmen zur Risikominimierung unternommen werden. Insbesondere wenn ein Unternehmen mit Cloud-Computing arbeitet, ist diese Vorschrift relevant. Denn beim Cloud-Computing wird oft mit größeren Mengen personenbezogener Daten hantiert. Noch stärker dürften Unternehmen betroffen sein, die Gesundheitsdaten speichern, gelten diese doch als besonders sensibel und eine Verbreitung der Daten wiegt für die Betroffenen besonders schwer.

- **Arbeitnehmerdaten**: Auf den Prüfstein kommt auch, wie ein Unternehmen die Daten seiner Arbeitnehmer bearbeitet. Die entsprechenden Regelungen in der DSGVO und dem BDSG-neu betreffen also auch die Human Resources, die in die Veränderungen miteinbezogen werden müssen.

- **Datenschutzbeauftragte**: Für viele Unternehmen ist ein Datenschutzbeauftragter fortan Pflicht. Dieser überwacht die individuell ausgearbeitete Datenschutzstrategie und die DSGVO/GDPR-Konformität. Das betrifft nicht bloß Unternehmen, die in großem Umfang mit personenbezogenen Daten arbeiten. Jedes Unternehmen, bei dem mehr als 10 Personen regelmäßig mit personenbezogenen Daten zu tun haben, muss künftig einen Datenschutzbeauftragten bestellen.

- **Meldepflichten**: Die neuen Vorgaben der DSGVO zum Vorgehen bei Datenpannen sind deutlich strenger als die zuvor geltenden Regelungen. Sicherheitsvorfälle müssen innerhalb von 72 Stunden nach Bekanntwerden gemeldet werden: Im Zweifel sowohl an die betroffenen Personen als auch an die zuständigen Behörden.

- **Verantwortlichkeit und Bußgelder**: Unternehmen können künftig für Verstöße im Umgang mit den von ihnen erhobenen Daten leichter verantwortlich gemacht werden. Das schließt hohe Geldbußen mit ein.

Sicherheit personenbezogener Daten

- **Dokumentationspflicht**: Ein Schwerpunkt der Datenschutzgrundverordnung liegt auf der Rechenschaftspflicht von Unternehmen, auch *Accountability* genannt. Anders als bisher sind Unternehmen verpflichtet, die Datenschutz-Compliance durch eine hausinterne Dokumentation belegen zu können. Sie müssen den Behörden jederzeit durch Vorlage eines entsprechendes Verzeichnisses darlegen können, welche Daten zu welchem Zweck gespeichert und auf welche Weise verarbeitet werden und wann das Unternehmen sie löscht.

- ***Privacy by Design***: Das Prinzip *Privacy by Design* bedeutet, dass Unternehmen bereits beim technischen Aufbau ihrer Geschäftsprozesse den Datenschutz berücksichtigen müssen. Sie dürfen Maßnahmen zum Datenschutz technisch nicht erst *nachträglich* (also zweitrangig) implementieren, sondern müssen sie bereits in der *Erarbeitungsphase* in den Arbeitsprozess integrieren. Produkte und Prozesse sollen also so konzipiert werden, dass sie mit möglichst wenig personenbezogenen Daten auskommen.

- ***Privacy by Default***: Diese Vorschrift der Datenschutz-Grundverordnung schreibt vor, dass grundsätzlich die datenschutz*freundlichste* Variante technisch voreingestellt sein muss. Das erspart es Verbrauchern, sich durch komplexe technische Einstellungen zu kämpfen, um Beschränkungen der Datenverarbeitung zu erwirken.

- **Erlaubnisgrundlagen (Einwilligung, Betriebsvereinbarung):** Auch künftig müssen Individuen der Nutzung ihrer persönlichen Daten in den meisten Fällen ausdrücklich zustimmen. Zudem ist die Einwilligung des Arbeitnehmers oder Verbrauchers nur für den anzugebenden Verwendungszweck gültig. Außerdem muss die Einwilligungserklärung verständlich formuliert und grundsätzlich widerrufbar sein. Der Widerruf muss für den Kunden ebenso einfach sein wie die Einwilligung. Die Anforderungen an eine wirksame Einwilligung sind nach der DSGVO gestiegen. Ein grobes Ungleichgewicht zwischen den Beteiligten kann die Freiwilligkeit ebenso ausschließen, wie die Kopplung der Erteilung an den Vertragsschluss.

- **Löschung von Daten**: Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für den Zweck notwendig ist. Erlischt die Verarbeitungsbefugnis (etwa weil die Einwilligung widerrufen oder der Vertrag erfüllt wurde), müssen die Daten gelöscht werden.

- **Auskunftsrecht und Recht auf Löschung**: EU-Bürger haben das Recht, auf Anfrage zu erfahren, über welche ihrer Daten ein Unternehmen verfügt und wie es diese verwendet. Außerdem können Verbraucher bei Unternehmen einfordern, ihre Daten zu löschen. Das „Recht auf Vergessenwerden" wird damit gesetzlich festgelegt.

Auswirkungen II: Webseitenbetreiber aufgepasst

Die Datenschutz-Grundverordnung enthält kaum explizite Regeln für den Onlinehandel. Sie formuliert vielmehr allgemeine Grundsätze des Datenschutzes, deren Teilbereiche in weiteren Gesetzen und Verordnungen geregelt werden. Dennoch bringen die abstrakten Normen der DSGV auch für den Onlinehandel einige Neuerungen. Mehr dazu erfahren Sie in den beiden folgenden Abschnitten.

Die Datenschutz-Grundverordnung ist gewissermaßen eine Übergangslösung: Denn ursprünglich sollte gemeinsam mit der Datenschutz-Grundverordnung noch eine weitere Neuregelung des Datenschutzes in Kraft treten: **die E-Privacy-Verordnung der EU**. Am 23.Oktober 2017 vom EU-Parlament beschlossen, ist dieser Zeitplan nun allerdings kaum noch einzuhalten. Es ist nämlich nicht zu erwarten, dass der Europäische Rat die Verordnung einfach so durchwinken wird: Der Entwurf sieht ein strenges Einwilligungserfordernis für Cookies vor. Würde dieser Entwurf Gesetz, hätte dies gravierende Auswirkungen auf Tracking, Targeting und personalisierte Werbung. Welche Änderungen hier im weiteren Gesetzgebungsprozess tatsächlich kommen werden, ist noch offen. Daher ist es derzeit zu früh, sich konkrete Gedanken über die E-Privacy-Verordnung zu machen – vor 2019 wird diese Verordnung wohl nicht wirksam. **Dennoch sollten Webseitenbetreiber und Onlinehändler die E-Privacy-Verordnung unbedingt im Blick behalten**. Denn im Gegensatz zur Datenschutz-Grundverordnung, die datenschutzrechtliche *Grundsätze* regelt, wird sich die E-Privacy-Verordnung auf einen sehr speziellen Bereich beziehen: den Schutz der Privatsphäre im digitalen Alltagsleben. Hier warten also weitere Neuregelungen auf Webseitenbetreiber.

Doch was ändert sich dann im Mai 2018 mit der Datenschutz-Grundverordnung der EU? Die wichtigsten Veränderungen für Webseitenbetreiber sind folgende:

- Die umfassende **Dokumentationspflicht** der Datenschutz-Grundverordnung
- Die komplexeren **Erlaubnistatbestände**
- Die Grundsätze von ***Privacy by Design*** und ***Privacy by Default***
- Erweiterte **Auskunftsrechte** und das **Recht auf Löschung**
- Das Recht auf **Datenübertragbarkeit**
- Deutlich umfangreichere Informationspflichten (z. B. für die **Datenschutzerklärung** einer Website)
- Das **Kopplungsverbot bei Einwilligungen**
- Sehr hohe **Bußgelder**

Einige Punkte haben wir in den vorherigen Abschnitten bereits erläutert. Die beiden Themen: **Datenschutzerklärung** und **Koppelungsverbot** werden im Folgenden dargestellt. Denn sie betreffen hauptsächlich Webseitenbetreiber.

Fakt

Datenschutz-*Einwilligung* und Datenschutz*erklärung* sind strikt zu unterscheiden. Die Einwilligung des Nutzers – erforderlich für jede Datenverarbeitung, die nicht durch eine Rechtsnorm erlaubt ist – meint die aktive Bestätigung eines Nutzers, dass er mit den Datenschutzbedingungen eines Unternehmens einverstanden ist. Die Datenschutzerklärung ist jener Text, in dem ein Unternehmen seinen Kunden seine Maßnahmen zum Datenschutz darlegt. Sie ist auf jeder Webseite Pflicht.

Die wichtigste Neuerung der DSGVO für Webseitenbetreiber stellen die Vorgaben zu den **Datenschutzbestimmungen** dar. Der Art. 13 Abs. 2 der DSGVO enthält einen ausführlichen Katalog von Informationen, die eine Datenschutzerklärung enthalten muss. Auch die Form die Datenschutzerklärung wird in der DSGVO deutlicher geregelt: Die Erklärung muss in verständlicher Sprache und inhaltlich nachvollziehbar erfolgen. Transparenz wird dabei in der DSGVO groß geschrieben.

Im **Kopplungsverbot** wiederum sehen Experten die größte Restriktion, die sich für die Netzwirtschaft aus der Datenschutz-Grundverordnung ergibt. Nach dem Kopplungsverbot darf ein Webseiten-Betreiber seine potenziellen Kunden künftig nicht zur Abgabe von Daten verpflichten, die für die eigentliche Leistung nicht notwendig sind. Ein Beispiel: Fordert man für das Zustandekommen eines Vertrages zugleich die Anmeldung für einen Online-Newsletter, so verstößt man künftig gegen EU-Recht. **Oberstes Prinzip der Einwilligung ist die Freiwilligkeit.** Vielen gekoppelten Einwilligungen dürfte jedoch die Freiwilligkeit fehlen. Die so eingeholten Einwilligungen sind folglich unwirksam.

Zuletzt noch einmal der **Hinweis**: Beachten Sie unbedingt die Änderungen zu Dokumentationspflichten, Erlaubnisgrundlagen, Speicherung, Auskunftsrechten und zum Recht auf Löschung. Im Einzelnen können auch weitere Neuregelungen Webseitenbetreiber und Unternehmen betreffen.

Maßnahmen: DSGVO-Checkliste für Unternehmen und Webseitenbetreiber

Möchte man mit der Umsetzung der neuen europäischen Datenschutz-Grundverordnung beginnen, gilt zunächst: Die erforderlichen Maßnahmen fallen je nach Unternehmen unterschiedlich aus. Dennoch gibt es eine Reihe an Vorkehrungen, die jedes Unternehmen berücksichtigen sollte. Wir haben diese in einer DSGVO-Checkliste für Sie zusammengefasst.

- Etablieren Sie **Dokumentationsprozesse** für den Umgang mit personenbezogenen Daten.
- Richten Sie ein **Verzeichnis der Verarbeitungstätigkeiten** ein.
- Richten Sie **Kommunikationsrouten für Kunden-Anfragen** zum Datenschutz ein.
- **Prüfen** Sie, **ob** Sie einen **Datenschutzbeauftragten** beauftragen müssen.
- Passen Sie die Datenschutzerklärung auf Ihrer Website an die Neuregelungen an.
- Beraten Sie sich mit dem Leiter Ihrer Technikabteilung und dem Datenschutzbeauftragten, ob die **aktuellen technischen Maßnahmen zum Datenschutz** ausreichen. Unter Umständen müssen weitere Maßnahmen eingeleitet oder bestehende Maßnahmen besser in die IT-Infrastruktur integriert werden.
- Alle erhobenen personenbezogenen Daten, die gegen das **Kopplungsverbot** verstoßen, müssen fortan anders eingeholt und als freiwillig ausgegebene Daten erhoben werden.
- Falls Sie externe Dienstleister damit beauftragt haben, personenbezogene Daten für Ihr Unternehmen zu verwalten, sollten Sie mit ihnen klären, ob die getroffenen **Vereinbarungen der Datenschutzreform entsprechen**. Passen Sie die Vereinbarungen gegebenenfalls den neuen Vorgaben an.
- **Überprüfen** Sie, wie Sie in Ihrem Onlineshop die **Einwilligungen Ihrer Kunden** einholen und passen Sie die Vorgehensweise an die Regelungen der Datenschutz-Grundverordnung an.
- **Bleiben Sie aufmerksam, was die E-Privacy-Verordnung angeht**: Sie wird künftig regeln, wie Onlinehändler mit Analyse- und Trackingtools umgehen.
- Falls Sie unsicher sind, wenden Sie sich bitte an **Ihre zuständige Kammer** oder nutzen Sie entsprechende **professionelle Beratung**.

Info-Quelle: https://www.1und1.at/digitalguide/websites/online-recht/datenschutz-grundverordnung-regeln-fuer-unternehmen/