Seit neun Monaten: verschärftes Datenschutzrecht

DSGVO
Die ersten Fälle und Erfahrungen

Die Angst war groß, seit rund neun Monaten ist das neue, verschärfte Datenschutzrecht nun in Österreich und EU-weit in Geltung. Wie hart werden Verstöße nun tatsächlich geahndet, und was sind die häufigsten Probleme? Im Folgenden die ersten Erfahrungen mit der DSGVO.

VON CHRISTIAN ZEILINGER* UND ANDREA WÜNSCHER

Strenge Dokumentationspflichten, Behördenchaos und viel Unmut: Die Datenschutzgrundverordnung hat im vergangenen Jahr EU-weit für reichlich Aufsehen gesorgt. Ein verlorener USB-Stick, ein unbedachter Anruf – ja sogar die eigene Website kann nun schnell zur Datenschutzfalle werden. Manche sind überzeugt, dass die Datenschutzgrundverordnung (kurz DSGVO) zu Recht in Österreich den wenig rühmenden Titel „Unwort des Jahres 2018“ trägt.

Einen Beitrag dazu leistete bisher wohl auch die Strafdrohung, die durchaus hellhörig macht: bis zu 20 Millionen Euro oder vier Prozent des Jahresumsatzes.

Durch die Verordnung, die EU-weit seit dem 25. Mai 2018 in Geltung getreten ist, müssen alle Unternehmen, Vereine und Behörden, die personenbezogene Daten verarbeiten, Vorkehrungen für den Schutz dieser Daten treffen. In Österreich sind also praktisch alle diese Organisationen verpflichtet, die DSGVO umzusetzen.

Hierzulande wurden bis dato lediglich vereinzelte Strafen ausgesprochen. Auch die Strafhöhe blieb bei den bekannt gewordenen Fällen deutlich unter dem möglichen Höchstbetrag. Unser Nachbarland legt bereits einen strengeren Maßstab an: Die deutschen Behörden prüfen laufend, ob auch die Vorschriften der DSGVO eingehalten werden. Vor allem das Bayerische Landesamt für Datenschutzaufsicht fordert derzeit Nachweise über die korrekte Umsetzung.

Was heißt das für heimische Unternehmen und Vereine? Auch in Österreich können die zuständigen Behörden jederzeit eine Dokumentierung der korrekten Einhaltung aller datenschutzrechtlichen Vorschrif-

*) Dr. Christian Zeilinger ist Rechtsanwalt in Oberösterreich mit den Schwerpunkten IT-Recht, Internet- und Datenschutzrecht sowie zertifizierter Datenschutzbeauftragter

ten verlangen. Und auch Beschwerden sind denkbar: Unter anderem kann in Bayern jedermann Datenschutzverstöße ganz einfach – sogar anonym – über eine Website melden. Auch Unternehmen mit Sitz in Österreich können so „angeschwärzt" werden.

Hartnäckige Mythen

Auch gut neun Monate nach Einführung der neuen Rechtslage kursieren noch immer viele Mythen rund um die neuen Regelungen.

1. Einwilligung & Löschung

Ein Mythos lautet: „Für die Verarbeitung personenbezogener Daten braucht man immer eine Einwilligung des Betroffenen." – Falsch! Allerdings ist eine Rechtsgrundlage für jede Verarbeitung zwingend erforderlich. Diese kann aber unter anderem auch durch eine Vertragserfüllung, eine gesetzliche Ermächtigung oder ein berechtigtes Interesse gegeben sein. Daher braucht man beispielsweise für die Zusendung einer Rechnung an einen Kunden oder das Speichern von Mitarbeiterdaten während eines aufrechten Arbeitsverhältnisses keine explizite Einwilligung der betroffenen Person.

Fällt der Zweck der Verarbeitung weg oder wird eine etwaige Einwilligung widerrufen, sind die Daten allerdings grundsätzlich umgehend zu löschen. Aber auch hier gibt es häufig Ausnahmen: Denn oft müssen Daten aus anderen Gründen länger gespeichert werden – ein ehemaliger Mitarbeiter kann beispielsweise bis zu 30 Jahre nach dem Ende des Arbeitsverhältnisses ein einfaches Dienstzeugnis verlangen. Dafür braucht man unter anderem allgemeine Daten zur Person, aber auch das Datum des Arbeitsbeginns und der Beendigung.

Auch die Aufbewahrungspflicht von Belegen und Geschäftspapieren ist zu beachten. Aus steuerlichen Gründen müssen Dokumente sieben Jahre aufgehoben werden, in Ausnahmefällen auch länger!

TIPP: Erstellen Sie ein Löschkonzept, wann welche Daten zu löschen sind!

2. Datenschutzbeauftragter

„Jedes Unternehmen benötigt einen Datenschutzbeauftragten?" Stimmt nicht! In Österreich muss ein Datenschutzbeauftragter nur bestellt werden, wenn die Kerntätigkeit des Unternehmens in der umfangreichen Verarbeitung von Daten liegt – wie z. B. bei Krankenanstalten, Banken oder Versicherungen. In den meisten Fällen ist ein Datenschutzbeauftragter also nicht zwingend erforderlich. Eine freiwillige Bestellung ist allerdings jederzeit möglich.

3. Werbeanrufe

„Ich darf eine im Internet veröffentlichte Telefonnummer nutzen, um neue Kunden zu akquirieren?" Nein! Ein erst-

Foto: SBphotos - Thinkstock.com, Bearbeitung: GEWINN

maliger Werbeanruf ohne vorherige Zustimmung war bereits vor der DSGVO in den meisten Fällen rechtswidrig. Doch nun hat auch die österreichische Datenschutzbehörde nach einer Beschwerde festgestellt: Eine auf einer Website zur Verfügung gestellte Telefonnummer zu Beratungszwecken darf nicht für Werbeanrufe verwendet werden, da es hierfür keine Rechtsgrund-

Achtung, ein Werbeanruf an eine im Internet kommunizierte Telefonnummer ohne vorherige Zustimmung ist rechtswidrig!

lage gibt und es damit auch der DSGVO widerspricht. Es ist demzufolge dringend von solchen sogenannten Cold Calls abzuraten.

Problemfall WhatsApp

Äußerst problematisch ist aber auch eine unternehmerische Nutzung von WhatsApp aus datenschutzrechtlicher Sicht. Denn was Vielen nicht bekannt ist: Der Messenger benötigt unter anderem den Zugriff auf das interne Adressbuch des Smartphones. Damit erhält der Konzern alle Telefonnummern des Nutzers der App – auch von den Personen, die den Messenger selbst gar nicht verwenden.

Diese Situation hat sich übrigens auch bei der seit etwa einem Jahr angebotenen „Business-Version" der App nicht verbessert: Mit dem Zustimmen der Nutzungsbedingungen werden sämtliche Kontakte an WhatsApp übermittelt. Bislang ist noch nicht bekannt, was mit diesen Daten in der Folge passiert.

Problematisch ist auch die Back-up-Funktion des Messengers. Möchte man den Chat-Verlauf, Bilder und Videos nicht nur intern auf dem Smartphone sichern, bietet WhatsApp auch die Möglichkeit einer Datensicherung auf Google Drive an. Der Haken an der Sache? Durch ein derartiges Back-up werden alle hochgeladenen Daten unverschlüsselt in der Cloud gespeichert. Google kann daher auf alle diese Daten zugreifen. Ein Verstoß gegen die DSGVO ist also sehr wahrscheinlich.

TIPP: Es gibt auf dem Markt bereits einige gute Alternativen, wie beispielsweise:

- Wire
- Threema
- Telegram
- Signal

Überhaupt ist es bei sämtlichen Apps ratsam, sich vor einer Installation über Rechtmäßigkeit, Berechtigungen, Verschlüsselung und Funktionsweise zu informieren.

Schwachstellen bei CMS

Die Verwendung von Content-Management-Systemen (CMS) wie „WordPress" oder „Joomla!" ist im Alltag vieler Betreiber von Websites nicht mehr wegzudenken, erleichtern sie doch erheblich die Erstellung und Verwaltung des Online-Auftritts.

Doch auch hier ist man bei falscher Nutzung schnell dem Risiko einer Abmahnung ausgesetzt. Regelmäßige Aktualisierungen aller Komponenten sowie ein vollständiges Impressum und eine Datenschutzerklärung sind Pflicht!

WhatsApp ist wohl auch in der „Business-Version" nicht DSGVO-konform

WICHTIG: Ist es bisher noch nicht passiert, sollte die eigene Website von Experten überprüft werden. So braucht es etwa eine Verschlüsselung über HTTPS und eine individuelle Datenschutzerklärung, die auf die technische Umsetzung der Website angepasst sein muss.

Viele Meldungen, erste Sanktionen

Dass der Datenschutz im Allgemeinen sowie auch die neue Verordnung ihre Berechtigung haben, zeigt die Anzahl der eingegangenen Beschwerden. Innerhalb der gesamten EU wurden bis Anfang September insgesamt 55.000 Beschwerden sowie rund 19.000 Meldungen von Datenschutzverletzungen gezählt. Auch die österreichische Datenschutzbehörde muss sich mit einer Fülle an Beschwerden befassen. Das Abarbeiten der zahlreichen Anfragen stellt die Behörde allerdings vor einige Herausforderungen.

Dagegen wird aber betroffenen Personen das Einbringen einer Beschwerde nicht leicht gemacht. Durch die Änderung des österreichischen Datenschutzgesetzes gibt es nun viele formale Kriterien zu erfüllen. Einfache Meldungen oder Anzeigen werden erst gar nicht mehr behandelt. Von einem vereinfachten Vorgang für Betroffene kann zumindest in Österreich – anders als zum Beispiel in Deutschland – wohl keine Rede sein.

Die bundesweit erste Geldbuße nach Inkrafttreten der DSGVO verhängte die Datenschutzbehörde aufgrund einer Videoüberwachung, die nicht korrekt gekennzeichnet war. Da eine Videoaufzeichnung auf Gehwegen oder anderen öffentlich zugänglichen Flächen nicht zulässig ist, musste der Betreiber eines Wettlokals in der Steiermark 4.800 Euro bezahlen.

Auch wenn in Österreich bislang nur eine Handvoll geringerer Geldbußen verhängt wurde, sind EU-weit bereits einige größere Verstöße gegen die DSGVO bekannt geworden. So machte etwa das Unternehmen, das den Flughafen Heathrow in London betreibt, Schlagzeilen. Im Oktober 2017 verlor ein Mitarbeiter einen USB-Stick, auf dem sich personenbezogene Daten befanden. Warum wird ein solcher Fehler bestraft? Die DSGVO fordert ein angemessenes Datenschutzniveau unter Berücksichtigung des Stands der Technik. Der Datenschutzverstoß hätte durch einen Passwortschutz des Datenträgers ganz einfach verhindert werden können. Er war aber nicht verschlüsselt und so konnten die Daten von jedem eingesehen werden.

Es wurde außerdem festgestellt, dass nur ein verschwindend geringer Pro-

zentsatz der Mitarbeiter eine Schulung im Bereich des Datenschutzes erhielten. Eine Mitarbeiterschulung ist allerdings von der DSGVO vorgesehen. Mit der Strafe in Höhe von 120.000 Pfund ist der Flughafen noch glimpflich davongekommen, da der Vorfall nach dem damals noch geltenden britischen Datenschutzgesetz beurteilt werden musste.

400.000 Euro Geldbuße

Die bislang höchste Strafe muss aber ein Krankenhaus in Portugal befürchten. Ganze 400.000 Euro wurden verhängt, da Patientendaten von zu vielen Mitarbeitern eingesehen werden konnten. In einem Krankenhaus zählen viele der Daten zudem auch zu den „sensiblen Daten", wie beispielsweise die Sozialversicherungsnummer oder die Krankengeschichte, und genießen daher besonderen Schutz.

WICHTIG: Auf die jeweiligen Daten dürfen nur diejenigen Personen Zugriff haben, die sie auch benötigen. Eine Liste mit den unterschiedlichen Zugriffsrechten im Unternehmen kann dabei hilfreich sein.

Hackerangriffe und die Folgen

Wie wichtig die Absicherung von Websites vor einem Hackerangriff ist, zeigt ein Fall aus Deutschland: Dort wurde ein Anbieter eines sozialen Netzwerks mit einer Geldstrafe belegt, da eine große Anzahl an Nutzerdaten von Cyberkriminellen ausgespäht und veröffentlicht wurde. Aufgrund der Tatsache, dass einige der Passwörter unverschlüsselt gespeichert wurden, kam es in der Folge zum Ausspruch einer Geldbuße in fünfstelliger Höhe.

Selbst die weltweit größten Hotelketten sind vor Angriffen nicht gefeit. Bis zu 500 Millionen Kundendaten sollen einem Tochterunternehmen des „Marriott" im November letzten Jahres gestohlen worden sein. Darunter Namen, Adressen, Passnummern und Kreditkarteninformationen. Obwohl letztgenannte Daten verschlüsselt gespeichert wurden, hat das Unternehmen die unangenehme Aufgabe, die betroffenen Kunden über die Datenpanne umgehend zu informieren. Ob der Vorfall auch eine Geldbuße aufgrund der DSGVO nach sich zieht, wird sich noch zeigen. Aber gewiss ist: Unternehmen müssen die DSGVO umsetzen und sich an die Regelungen halten, wenn sie personenbezogene Daten von EU-Bürgern verarbeiten – auch wenn ihr Sitz in einem Drittstaat liegt.

Die DSGVO richtig umsetzen

Was kann man nun tun, um der Verordnung zu entsprechen? Wichtig ist es, sich umfangreich zu informieren, da in jedem Unternehmen unterschiedliche Maßnahmen ergriffen werden müssen. Die DSGVO wird oft als notwendiges Übel gesehen, aber bei richtiger Anwendung der Vorschriften gewährleistet sie Schutz der heutzutage äußerst wertvollen personenbezogenen Daten und trägt auch zur Transparenz bei. Ein weiterer Vorteil, den die Verordnung mit sich bringt: Sie schafft ein Bewusstsein für eventuell überflüssige Prozesse oder nicht mehr benötigte Software und zeigt damit auch Kosteneinsparungen auf. Auch kann eine offene Präsentation der Kooperationspartner, welche die Daten in weiterer Folge verarbeiten, einen Marketing-Zweck für ebenjene erfüllen und positives Netzwerken begünstigen.

Und wenn doch etwas passiert? – Auch dafür sollte man sich rüsten, um schnell reagieren zu können: Datenpannen müssen in der Regel innerhalb einer kurzen Frist selbst bei der zuständigen Datenschutzbehörde angezeigt werden. Davon abgesehen werden darf nur, wenn z. B. bei einem verlorenen Notebook oder einer Festplatte mithilfe sicherer Verschlüsselung ein Zugriff durch Dritte nicht möglich ist.

Fällt der Zweck der Verarbeitung weg oder wird eine Einwilligung widerrufen, sind die Daten grundsätzlich zu löschen. Es sei denn, andere Pflichten stehen entgegen, etwa die siebenjährige steuerliche Belegaufbewahrungspflicht

Fotos: nicomenijes - Thinkstock.com