Foto: Shutterstock / Kb-photodesign; Ket4up

Die letzten drei Monate

Ende Mai tritt die neue EU-Datenschutz-Grundverordnung in Kraft. Was können Unternehmen, die sich darauf bislang nicht vorbereitet haben, jetzt noch tun?

16 Jahre: Mindestalter für das wirksame Einwilligen in die Verarbeitung personenbezogener Daten

Quelle: MIP Consult GmbH

Es hat an Hinweisen nicht gefehlt: Seit über einem Jahr thematisieren Anwälte, Verbände und nicht zuletzt Fachmedien die EU-Datenschutz-Grundverordnung (DSGVO). Vor über einem Jahr schrieb der Autor in diesem Heft (Ausgabe 1/17) „DSGVO: Die Zeit drängt" – ein Hinweis darauf, dass etwas mehr als ein Jahr für die Umsetzung der nach der EU-Datenschutz-Grundverordnung erforderlichen Prozesse und Dokumentationspflichten schon recht knapp bemessen ist.

Doch vielen Unternehmen scheint der Ernst der Lage nicht bewusst zu sein. Aktuell melden sich viele Klienten in der Kanzlei des Autors, die – offenbar mit großem Vertrauen in ihre Leistungsfähigkeit gesegnet – sich erst jetzt so richtig mit der Umsetzung der Datenschutz-Anforderungen befassen. In der Regel handelt es sich dabei um mittelständische Unternehmen. Viele Geschäftsführer und Vorstände beginnen zu erkennen, dass die DSGVO nicht nur ein zahnloser Bürokratie-Tiger ist, sondern sowohl Gesetzgeber als auch Behörden es ernst mit der Einhaltung des Datenschutzes meinen. Und die Manager sind alarmiert, denn bei Datenschutzverstößen können sie persönlich haftbar gemacht werden.

Eine datenschutzkonforme Umsetzung aller Themen und Prozesse im Unternehmen innerhalb von drei Monaten dürfte in der Regel kaum noch darstellbar sein. Doch was lässt sich bis zum 25. Mai noch bewältigen? Dieser Artikel soll dabei helfen, über einen Maßnahmenplan strukturiert und effektiv zu handeln, um wenigstens die größten datenschutzrechtlichen Fehler und damit die immer wieder zitierten Bußgelder zu vermeiden. Und die können schmerzliche Dimensionen erreichen. Es drohen bei mittelschweren Verstößen Bußgelder von bis zu zwei Prozent des jährlichen Konzernumsatzes oder bis zu zehn Millionen Euro. Bei schweren Verstößen können diese verdoppelt werden.

Wahrscheinlich werden Datenschutzbehörden bei der Verhängung von Bußgeldern nicht lange fackeln, da vom Inkrafttreten bis zur Umsetzung durchaus Zeit war, datenschutzkonforme Systeme zu etablieren. Das Kohärenzprinzip wird dazu führen, dass Datenschutzbehörden in Europa einheitlich Bußgelder verhängen werden, sodass nicht zuletzt auch hier mit

DSGVO-Checkliste

1. Die Bestandsaufnahme

Wo im Unternehmen werden personenbezogene Daten erfasst, verarbeitet oder gespeichert?

Welche Systeme werden hierfür eingesetzt? Welche Personen haben Zugriff auf die Daten?

Welchen Zweck erfüllen die erhobenen Daten? Sind die erhobenen Daten für diesen Zweck erforderlich?

Werden die Grundsätze von Privacy by Design und Privacy by Default eingehalten?

2. Die Dokumentation

Welche Prozesse durchlaufen die Daten?

Welche Zugriffsberechtigungen gibt es? Welche Mitarbeiter haben Zugang zu den Daten?

Welche externen Auftragsverarbeiter sind involviert? Wie gewährleisten diese die Einhaltung des Datenschutzes?

Nach welchem Konzept werden Daten gelöscht?

Wie sieht das Meldekonzept bei Datenschutzverstößen aus?

3. Das Team

Alle Abteilungen, in denen personenbezogene Daten verarbeitet werden, müssen eingebunden werden.

Gibt es einen Datenschutzbeauftragten? Braucht das Unternehmen einen solchen?

Gibt es einen Betriebsrat? Gibt es Betriebsvereinbarungen?

Reichen die eigenen Kompetenzen im Haus aus, um die Aufgaben abzuarbeiten. Sonst sollten externe Experten hinzugezogen werden.

verschiedenen „Leuchtturm"-Verfahren mit abschreckenden Bußgeldern zu rechnen sein wird.

Der Umfang der Maßnahmen, die umgesetzt werden müssen, hängt davon ab, in welchem Geschäftsbereich ein Unternehmen tätig ist, welche Art von Daten, insbesondere sensible Daten, verarbeitet werden und auch wie groß die Sichtbarkeit bestimmter Prozesse nach außen ist. Es spielt auch eine Rolle, ob ein Unternehmen beispielsweise als IT-Dienstleister für Kunden agiert.

Bezogen auf Webportale und Online-Shops bedeutet dies: Sie verarbeiten personenbezogene Daten von Nutzern, daher sind sämtliche Anforderungen an Datenschutzerklärungen, Anforderungen bezüglich einer informierten Einwilligung bis hin zu Löschungskonzepten – und Informationen darüber – rechtzeitig umzusetzen.

Webshop-Betreiber, die sich nicht datenschutzkonform verhalten, müssen nicht nur mit Ärger von den Datenschutzbehörden und von etwaigen Mitbewerbern rechnen, die etwaige Verstöße anprangern und Abmahnungen schicken. Über die „klassischen" Bußgeldtatbestände hinaus sei auch auf das nunmehr kodifizierte Recht verwiesen, aus dem sich die Forderung nach materiellem oder immateriellem Schadensersatz gegen Verantwortliche oder auch deren Auftragsverarbeiter ergibt. Es besteht somit zu befürchten, dass es hier zu einer Vielzahl von Einzelverfahren gegen ein Unternehmen kommen kann, verhält dieses sich nicht datenschutzkonform.

Bußgelder bei Verstößen auch gegen die Dienstleister

Wichtig ist für alle Beteiligten auch zu wissen, dass nicht nur das Unternehmen selbst, sondern nach neuem Recht auch der Auftragsverarbeiter für die Einhaltung datenschutzrechtlicher Vorschriften haftet. Während sich früher IT-Dienstleister als Auftragsverarbeiter (früher Auftragsdatenverarbeiter genannt) noch zurücklehnten, weil die Haftung den Auftraggeber traf, so können nun dieselben Bußgelder bei Datenschutzverstößen auch gegen die Auftragsverarbeiter verhängt werden. Jeder Dienstleister, erst recht jeder Hoster, ist also gut beraten, sich um den Datenschutz seiner Kunden zu kümmern.

Was ist in der verbleibenden Zeit noch möglich?

Zunächst bedarf es einer dezidierten Risikoanalyse mit einer Bestandsaufnahme von Prozessen und Verfahren. Jedes Unternehmen hat zu untersuchen, welche Daten über welche Systeme verarbeitet werden. Gemeint ist hier tatsächlich die Verarbeitung auf Datenfeldebene, da sich hier bereits die Frage der Notwendigkeit für den relevanten Zweck ergibt. Unter den Schlagwörtern Privacy by Design und Privacy by Default ist nämlich gemeint, ▶

Datenschutz-Grundverordnung: Die Fakten

Worum geht es?
Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarkts gewährleistet werden.

Der Vorgänger
Die DSGVO ersetzt eine EU-Verordnung über die Verarbeitung von personenbezogenen Daten aus dem Jahr 1995.

Wann geht's los?
Die Verordnung wird am 25. Mai 2018 wirksam. Eine Übergangsfrist ist nicht vorgesehen. Ein Anpassungsgesetz aus dem Jahr 2017 hat dafür gesorgt, dass ab dem Stichtag das Bundesdatenschutzgesetz DSGVO-kompatibel ist.

Wen betrifft es?
Jedes Unternehmen, das personenbezogene Daten von EU-Bürgern verarbeitet oder speichert, egal ob in eigenem oder fremdem Auftrag.

E-Privacy
Oft in einem Atemzug genannt, sind die DSGVO und die E-Privacy-Verordnung dennoch nicht dasselbe. Bei der E-Privacy-Richtlinie geht es um das Erheben, die Weitergabe und den Austausch personenbezogener Daten (Stichworte: Profilbildung, Tracking, Targeting). Die E-Privacy-Verordnung ist noch nicht verabschiedet, es kann noch mehrere Jahre dauern, bis sie Gültigkeit erlangt.

Die Geschichte der DSGVO

Juni 2013

Ein Entwurf für ein neues, europaweites Datenschutzgesetz, der von der irischen Ratspräsidentschaft vorgelegt wurde, scheitert nach langen Verhandlungen im EU-Ministerrat.

März 2014

Das EU-Parlament einigt sich auf eine gemeinsame Verhandlungsposition.

Juni 2015

Die EU-Justizminister einigen sich ebenfalls auf eine gemeinsame Verhandlungsposition für einen abgeschwächten Entwurf.

Dezember 2015

EU-Ministerrat und -Parlament einigen sich auf einen Entwurf.

April 2016

EU-Ministerrat und EU-Parlament verabschieden die DSGVO.

Mai 2016

Die DSGVO wird im Amstblatt der EU veröffentlicht und tritt zwei Wochen später in Kraft. Damit einher geht eine zweijährige Zeitspanne, ab der die Verordnung in den Mitgliedsländern anzuwenden ist.

25. Mai 2018

Die Frist läuft ab. Die DSGVO muss angewendet werden.

dass der Verantwortliche den Datenschutz durch datenschutzfreundliche Voreinstellungen sicherzustellen hat, dass nur die personenbezogenen Daten verarbeitet werden, die für den konkreten Zweck erforderlich sind.

Bei Online-Shops stellt sich vor diesem Hintergrund die Frage, welche Datenfelder tatsächlich für einen Bestellvorgang gerechtfertigt sind. Kennt man den Umfang der personenbezogenen Daten und Datenfelder, ist zu untersuchen, auf welchen Systemen mit welcher IT-Architektur diese verarbeitet werden, vor allem durch wen – und wer darauf Zugriff hat.

Ebenfalls erforderlich ist die Schaffung eines Datenschutzmanagementsystems, das umfangreiche Anforderungen an die Dokumentation und Implementierung von Regeln, Prozessen und Maßnahmen enthält. Ohne alle zu nennen, gehört hier das Verzeichnis von Verarbeitungstätigkeiten und das IT-Sicherheitsmanagement genauso dazu wie ein Berechtigungs-, ein Löschungs- oder auch ein Meldekonzept bei Datenschutzverstößen. Weitgehend unbeachtet ist bislang der als Ergänzung zur DSGVO neu aufgenommene § 77 BDSG, wonach der Verantwortliche eine Möglichkeit schaffen muss, dass ihm vertrauliche Meldungen über Datenschutzverstöße zugeleitet werden müssen, also eine Whistleblower-Vorschrift.

Dokumentation und Rechenschaftspflicht

Setzt man sich also mit den Grundanforderungen an Dokumentationspflichten mit den genannten Aspekten auch des Datenschutzrisikomanagements auseinander, sollte eine Task Force zusammengestellt werden, die sich als Projektteam nunmehr konzentriert mit der Umsetzung der DSGVO beschäftigt.

Hier bedarf es neben der Festlegung von Projektzielen und der Bestandsaufnahme auch einer Gap-Analyse, das heißt eines strukturierten Abgleichs des Ist-Zustands mit dem Soll-Zustand. Dieses Projektteam muss den Datenschutzbeauftragten einbinden, gegebenenfalls auch den Betriebsrat; etwaige Betriebsvereinbarungen sind anzupassen.

Sobald die Handelnden und deren Verantwortlichkeiten definiert und über die Gap-Analyse der Anpassungsbedarf ermittelt wurde, geht es in die Planung neuer Prozesse und Strukturen, zumindest aber an die Ad-hoc-Anpassung der Einzelprozesse.

Externe Leistungen und Auftragsverarbeitung

In der Praxis zeigt sich immer wieder, dass, sei es durch Pflege und Support, sei es durch Hosting oder auch durch Nutzung externer Software as a Services, personenbezogene Daten von Dritten verarbeitet werden. Hier handelt es sich regelmäßig um Auftragsverarbeiter im Sinne von Artikel 28 DSGVO. Diese Auftragsverarbeiter müssen, wie der Verantwortliche auch, bestimmte Sicherheitsanforderungen bezüglich der Verarbeitung gewährleisten, allen voran technische und organisatorische Maßnahmen (kurz „TOMs“). Artikel 28 Absatz 3 schreibt vor, dass eine Verarbeitung durch einen Auftragsverarbeiter auf Grundlage eines Vertrags zu erfolgen hat, der insbesondere die in diesem Absatz genannten Regelungsinhalte aufweist. Hier sollte jedes Unternehmen große Sorgfalt walten lassen, insbesondere dann, wenn es sich um außereuropäische Unternehmen handelt. Während man bei der durch den Verantwortlichen selbst durchzuführenden Risikoeinschätzung durchaus bei einzelnen „Stellschrauben“ zur Bewertung der Risiken noch unterschiedlicher Auffassung sein kann, lässt sich über das Erfordernis und den Inhalt einer Vereinbarung über Auftragsdatenverarbeitung auch mit der dann zuständigen Datenschutzbehörde nicht ernsthaft diskutieren. Speziell solche Themen werden sicherlich in Zukunft sehr aufmerksam beobachtet und im Verletzungsfalle unmittelbar mit spürbaren Bußgeldern sanktioniert werden.

4.000
Änderungswünsche wurden im gesetzgeberischen Verfahren in die DSGVO eingearbeitet

Quelle: MIP Consult GmbH

Risikopriorisierung in der verbleibenden Zeit

Entsprechend der Risikopriorisierung über die Höhe von zu erwartenden Bußgeldern sollten die Verantwortlichen in der verbleibenden Zeit realistisch definieren, welche Gegenstände der Datenverarbeitung als kritisch einzustufen sind, und diese entsprechend hoch priorisieren. Dies kann beispielsweise zunächst einmal die umfangreich zu fordernde Dokumentation des Datenschutzmanagementsystems mit ihren einzelnen Inhalten wie Verfahrensverzeichnis, Sicherheitskonzept, Berechtigungskonzept, Löschungskonzept, Meldekonzept oder bei sensiblen Daten auch die Datenschutz-Folgeabschätzung sein.

Bei Unternehmen mit mehr als 10 Personen, die mit der Datenverarbeitung betraut sind, muss ein Datenschutzbeauftragter benannt werden: Er sollte hier vollständig mit einbezogen werden.

Es empfiehlt sich weiter, die entsprechenden Unterlagen auch so aufzubereiten und zu versionieren, dass diese für die jeweiligen Prozesse effektiv fortgeschrieben werden können. Erste Angebote von Tools finden sich hierzu im Markt. Zu überlegen ist auch zur Abfederung fehlender Skills und/oder Ressourcen, hier externe Berater einzubeziehen. Mit Blick auf die hohen Bußgeldandrohungen dürfte deren Vergütung relativ günstig sein.

Sind dann die Gegenstände höchster Priorität umgesetzt, um wenigstens gravierende Verletzungstatbestände möglichst vollständig zu vermeiden, geht es in einem zweiten Schritt um die Anpassung der im Rahmen der Gap-Analyse noch offenen Themen.

Natürlich ist die Zeit knapp, aber ein mittelständisches Unternehmen kann es durchaus noch schaffen, bis zum Stichtag des Inkrafttretens die wesentlichen Datenschutzthemen abzuarbeiten, um zumindest weitestgehend datenschutzkonform am Markt tätig sein zu können. Dies erfordert indes ein konzentriertes und fokussiertes Vorgehen mit einem gut organisierten und fachlich versierten Team. Abwarten und Tee trinken ist dagegen die falsche Strategie. Denn einem Unternehmen, das so handelt, werden die Datenschutzbehörden im Falle gravierender Datenschutzverstöße wahrscheinlich nicht mehr Fahrlässigkeit zubilligen, sondern Vorsatz unterstellen. ■

Dr. Hajo Rauschhofer
ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht. Zu seinen Tätigkeitsschwerpunkten gehören außerdem Internet-Recht sowie Marken- und Medienrecht.
www.rechtsanwalt.de

Cloud-Computing und Datenschutz

Die DSGVO gilt für jeden, der personenbezogene Daten von EU-Bürgern verarbeitet oder verarbeiten lässt – die Speicherung in einer Cloud oder die Verarbeitung mit einer SaaS-Lösung gehört dazu. Wer Daten von EU-Bürgern außerhalb der EU verarbeiten lässt, muss dafür Sorge tragen, dass auch dabei die EU-Datenschutzgrundsätze eingehalten werden.

Unternehmen, die mit externen Datenpartnern innerhalb der EU zusammenarbeiten, müssen ihre ADV-Verträge anpassen. Anders als bisher ist nur noch ein Auftrag zur Datenverarbeitung erforderlich, die Verarbeitung muss nicht mehr weisungsgebunden sein. Und: Nicht mehr der Auftraggeber allein haftet, auch für den Dienstleister gelten jetzt gesetzliche Pflichten. Bei einer Datenverarbeitung außerhalb der EU sollten Unternehmen die EU-Standardvertragsklauseln oder Binding Corporate Rules nutzen, die von den Aufsichtsbehörden genehmigt wurden. Diese gelten, seit im Sommer 2016 das EU-US-Privacy-Shield-Abkommen geschlossen wurde.

Wichtig: Für dieses Abkommen gibt es derzeit noch keinen Nachfolger, deshalb müssen entsprechende Verträge nicht geändert werden. Dies kann sich aber jederzeit ändern, deshalb sollten betroffene Unternehmer die Entwicklung aufmerksam verfolgen.

Eine Überlegung wert ist es, bei Cloud-Lösungen auf eine wirksame Verschlüsselung zu achten.