Sehr geehrte Damen und Herren,
liebe Kundinnen und Kunden,

seit Ausbruch der Corona-Pandemie und den eingeleiteten staatlichen Restriktionen sind nun einige Wochen vergangen. Durch die große Disziplin der Menschen konnte ein massiver Anstieg von Infektionen deutlich gebremst werden.

Die allermeisten von uns haben sich inzwischen auf die neue Situation in ihrem privaten wie geschäftlichen Leben eingestellt. Die Lockerungen des Lockdowns schaffen Räume, wieder Wege in die „Normalität“ zu denken und zu gehen. Das gilt auch für das Datenschutzteam der mip. Dabei blenden wir die Erfahrungen der Sondersituation nicht aus. Wir sehen hierin einen Erfahrungsschatz, den wir für uns, aber natürlich auch für unsere Kunden nutzen wollen.

Daher haben wir die Datenschutzthemen, die für das „Hochfahren“ eines Unternehmens relevant sein können, aufbereitet. Hier gibt es insbesondere beim Beschäftigtendatenschutz, als auch bei Dienstleistungen mit Kundenkontakt diverse neue Vorgaben zu beachten oder Organisationsabläufe etc. zu überdenken und anzupassen.

Da die Experten noch immer von einer zweiten Welle im Herbst ausgehen, gilt der alte Fußballergrundsatz: „Nach dem Spiel ist vor dem Spiel!“ Wie empfehlen daher jetzt, das bestehende Notfallmanagement im Unternehmen zu hinterfragen, um dafür rechtzeitig und mit Vorlauf falls notwendig auf neue, stabilere und rechtssichere Beine zu stellen.

Und natürlich haben wir einige Praxisthemen für Sie zusammengestellt, die trotz Corona aktuelle Relevanz für den täglichen Geschäftsbetrieb haben.

Wir bleiben also für Sie und mit Ihnen am Ball und wünschen Ihnen weiterhin: Bleiben Sie gesund!

Ihr

Asmus Eggert

Inhalt

Corona-Pandemie: Hochlauf nach dem Lockdown – Was ist zu beachten?

Nach und nach werden die Restriktionen des Lockdowns durch die staatlichen Stellen gelockert. Die Unternehmen stehen vor einer neuen Herausforderung, dem Hochlauf. So wenig wie der Datenschutz beim Lockdown außer Kraft gesetzt wurde, so wenig ist dies beim sog. Hochlauf der Fall. Der wesentliche Unterschied besteht darin, dass der Lockdown für alle überraschend kam und vielfach Maßnahmen adhoc notwendig waren. Diese waren in der Regel als Gesundheitsschutz, der Fürsorge für die Beschäftigten oder zur Aufrechterhaltung eines Notbetriebes für eine bestimmte Zeit im Rahmen einer Risikoabwägung zu rechtfertigen. Das war auch den Hinweisen der Aufsichtsbehörden zu entnehmen, die vielfach gute Vorlagen, Muster und Hinweise veröffentlicht haben. Auch wir hatten in unserer letzten Beraterinfo Corona zum Schwerpunktthema gemacht.

Der sog. Hochlauf steht jedoch unter der Maxime der „Bedächtigkeit“ und die allgemeine Erwartungshaltung ist, dass er organisiert vorbereitet und umgesetzt wird. Die Diskussionen über den richtigen Weg der Lockerungen führen dabei zu unterschiedlichen Regelungen in den einzelnen Bundesländern. Es ist deshalb zu prüfen, welche Regelungen konkret für den Standort oder ggfs. die Standorte eines Unternehmens gelten und ob bzw. inwieweit diese einheitlich umgesetzt werden können. Diese Rahmenbedingungen werden zu individuellen Lösungen führen.

Praxishinweis: Vielfach müssen oder sollen Listen geführt werden, die personenbezogene Daten enthalten. Dazu gehören Anwesenheitslisten von Mitarbeitern im Büro, um z.B. sicherzustellen, dass eine bestimmte Anzahl von Personen im Büro nicht überschritten wird. Auch werden Mitarbeiter aufgefordert, eigene Gesundheitsdaten zu erfassen (z.B. ein täglich geführtes Journal über Körpertemperatur und weitere Corona-Virus-Symptome), wobei sich die Frage stellt, ob dies zulässig ist und wer auf diese Daten Zugriff haben darf. Oder es müssen aufgrund gesetzlicher Regelungen Verfahren bzw. Dokumentationen um- und eingesetzt werden, die eine Nachverfolgbarkeit von Ansteckungsketten bei den Besuchern ermöglicht (z.B. in Gastronomie- und Friseurbetrieben).

Beim Führen solcher Listen gelten weiterhin die bekannten Grundsätze: Die Personen sind über Inhalt und Zweck der Datenerhebung zu informieren, es ist sicher zu stellen, dass keine unberechtigten Personen auf die Daten zugreifen können (Tabellen, in denen sich Gäste untereinander eintragen, genügen dieser Anforderung nicht!). Soweit Bundesländer in den jeweiligen Corona-Verordnungen Löschfristen bestimmt haben (Nachverfolgungslisten für Infektionsketten in der Regel 4 Wochen), sind die die Daten nach Ablauf dieser Frist zu löschen. Gibt es keine Regelung, sind die Daten nach Wegfall des Zwecks zu löschen. Wenn Sie hier Unterstützung brauchen, wenden Sie sich gerne an Ihren Berater des mip Datenschutzteams.

Der Notfallplan – Die drei kleinen Schweinchen und ihr Notfallmanagement

„Es waren einmal drei kleine Schweinchen Milly, Billy und Willy. Milly, das erste Schweinchen baute sein Haus aus Stroh, denn es lebte ja so froh. Billy, das zweite Scheinchen baute sein Haus aus Holz, darum war es ja so stolz. Das dritte Schweinchen Willy baute sein Haus aus Stein, denn haltbar musste es sein.

Milly und Billy bauten ihre Häuser sehr schnell. Billy, das dritte Schweinchen jedoch, arbeitete den ganzen Tag hart, um sein Haus aus Stein so stabil wie möglich zu bauen, denn er hatte große Angst vor dem bösen Wolf.

Eines Tages entdeckte der böse Wolf die singenden und tanzenden Schweinchen. Er bedrohte den kleinen Milly und Billy. Sie liefen ängstlich in ihre Häuser und versteckten sich vor ihm. Zuerst ging der Wolf zu dem Haus aus Stroh. Er strampelte, trampelte, hustete und pustete bis das Strohhaus zusammenfiel. Der verängstigte Milly konnte jedoch in Billys Holzhaus flüchten und sich retten. Daraufhin schaffte der böse Wolf ebenfalls mit wenig Mühe, auch das Holzhaus nieder zu pusten. Die beiden ängstlichen Schweinchen rannten mit aller Kraft davon und kamen bei Willy im Steinhaus

unter. Der böse Wolf versuchte nun auch mit aller Kraft das Steinhaus nieder zu pusten, doch dieses hielt stand, der Wolf gab schließlich auf und lief kraftlos davon.

Milly und Billy bereuten sehr, die Gefahr nicht richtig eingeschätzt zu haben und bauten in Vorbereitung für zukünftige Gefahren, mit der Unterstützung und dem Knowhow von Willy, ebenfalls stabile Häuser aus Stein und lebten glücklich bis ans Ende ihrer Tage."

Die Lektion dieses Märchens indiziert die aktuelle Relevanz und Priorität einer guten Vorbereitung für Sondersituationen. Die vergangenen Monate haben gezeigt, wie schnell eine vorher nie dagewesene Ausnahmesituation zu einer ernstzunehmenden Gefahr für Unternehmen und deren Beschäftigten führen kann und in einzelnen Fällen schon geführt hat.

Eine Pandemie zählt – so unser aller Hoffnung - zu einer eher seltenen Ausnahmensituation für ein Unternehmen. Viel wahrscheinlicher realisieren sich allerdings andere, oft alltägliche Risiken und Gefahren und bringen so Unternehmen in Schwierigkeiten: Stromausfall, Ausfall des Haupt- oder des einzigen Lieferanten, Naturkatastrophen, Diebstahl, etc. Die Szenarien sind vielfältig. Durch Digitalisierung und Vernetzung gewinnen jedoch der Ausfall oder die Einschränkung des Internets sowie das Thema Cyberkriminalität an Bedeutung. Diesen Trend zeigen recht eindeutig die Ergebnisse des Lageberichts zur IT-Sicherheit 2019 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie diverse andere Studien. Die Ausfälle der IT-Infrastruktur in Verbindung mit Datenverlusten steigen in Unternehmen enorm an. Hackerangriffen nehmen deutlich zu. Erschreckend ist, dass trotz alledem eine Vielzahl der Unternehmen nichts unternimmt, um den Schutz vor solchen Ausfällen und Angriffen zu erhöhen. Oft wird erst reagiert, wenn es zu spät ist und ein Schaden entstanden ist.

Die globale Extremsituation der Corona-Pandemie hat offenbar jedoch den Effekt, dass sich immer mehr Unternehmen mit dem Thema „Notfall-Management" beschäftigen. Ein Datenschutzkonzept beinhaltet dabei bereits gute Ansätze, mit denen sich ergänzend ein IT-Notfallplan erarbeiten lässt, um sich zukünftig für derartige Situationen mit einer passenden Strategie zu wappnen. Zum Beispiel sind in den technischen und organisatorischen Maßnahmen (TOM) sowie im Incident-Response-Management entsprechende Regelungen und Verfahren für die Sicherung personenbezogener Daten hinterlegt. Hieraus resultierend wurden Prozesse geschaffen und implementiert, die z.B. der Absicherung vor unbefugten Zugriffen dienen und eine dauerhafte Verfügbarkeit personenbezogener Daten gewährleisten. Diese Logiken können vielfach auf den Schutz für alle Daten im Unternehmen, insbesondere Daten über Unternehmensprozesse, Produktionsdaten und -prozesse, Patente u.v.m. übertragen werden.

Ohne ein implementiertes Notfallmanagement entstehen Kausalitätsketten, die Sie und Ihre Partnerunternehmen in existenzielle Probleme führen können. Dies heißt es zu vermeiden, denn der Schutz von Arbeitsplätzen, die Vermeidung hoher Umsatzeinbußen, Rechtsverletzungen sowie von Reputationsschäden besitzen höchste Priorität.

Mithilfe eines zielgerichteten Notfallmanagements können Sie vorbereitet und entschlossen auf Sondersituationen, wie IT-Ausfälle, Lieferengpässe oder eben auch Pandemien reagieren und mit entsprechenden Strategien aktiv handlungsfähig bleiben.

Wie können Sie das Thema angehen?

Mit unserem interdisziplinären Team bestehend aus Juristen, Informationssicherheitsbeauftragten, Risiko- und BCM- Managern haben wir ein ***Notfall-Management*** ***check-up!*** entwickelt, um kritische Geschäftsprozess sowie Handlungsfelder aufzudecken. Diesen ersten ***check-up!*** bieten wir Ihnen als Bestandskunde für **2.500 EUR** an. Wer sich bis zum 15.07.2020 meldet, profitiert von dem Frühbucherrabatt und zahlt nur **2.000 EUR**.

Wir laden Sie ein, uns anzurufen oder uns eine E-Mail zu schreiben und sich direkt mit Ihren Rückfragen und Wünschen bei uns zu melden. Wir sind für Sie da!

Ganz in dem Sinne: Mit einem Notfall-Management kann der Wolf noch so viel strampeln, trampeln, husten und pusten – Sie sind vorbereitet!

BGH zum Cookie-Banner: Voreingestelltes „Ja“ ist keine aktive Einwilligung!

Der Bundesgerichtshof (BGH) hat mit seiner Entscheidung vom 28.05.2020 (I ZR 7/16 - Cookie-Einwilligung II) die Anforderungen an die Einwilligung in telefonische Werbung und Cookie-Speicherung klargestellt.

Gegenstand der Entscheidung war der Fall, dass in einem Formular das Ankreuzfeld für die Einwilligung in die telefonische Werbung und die Cookie-Speicherung bereits vom Anbieter der Webpage vorausgefüllt war.

Der BGH hat nun entschieden, dass dieses voreingestelltes Ankreuzkästchen, das der Nutzer zur Verweigerung seiner Einwilligung abwählen muss, den gesetzlichen Anforderungen an eine aktive Einwilligung nicht genügt. So stelle das Betätigen einer Schaltfläche für die Teilnahme am Gewinnspiel deshalb noch keine wirksame Einwilligung des Nutzers in die Speicherung von Cookies dar. D. h., notwendig ist ein aktives Verhalten des Nutzers. Er müsse ohne jeden Zweifel und freiwillig handeln.

Das kommt Ihnen möglicherweise bekannt vor. Das liegt daran, dass dies der Europäische Gerichtshof (EuGH) bereits am 01.10.2019 in einem sog. Vorabentscheidungsverfahren (Az.: C-673/17) entschieden hatte. Wir hatten Sie darüber bereits informiert und auch einen Blog-Beitrag geschrieben. Der BGH hatte sein Verfahren zur Vorlage beim EuGH im Jahr 2017 ausgesetzt und legt nun die EuGH-Entscheidung seinem Urteil zugrunde. Damit bringt er den Fall nun zum Abschluss.

Tatsächlich hinterfragen IT-Konzerne (Google etc.) inzwischen ernsthaft den Einsatz von Cookies und entwickeln technische Alternativen, um an die bisher über Cookies gewonnenen Informationen zu kommen. Das bedeutet jedoch nicht, dass diese Informationen nun ohne Einwilligung gesammelt werden können. Das dürfte nun durch den BGH mit seiner europarechtskonformen Auslegung dieser telekommunikationsrechtlichen Situation aus dem Telemediengesetz (TMG) klargestellt sein. Wir gehen derzeit davon aus, dass sich das auch in der noch immer ausstehenden e-Privacy-Verordnung wiederfinden wird.

Praxishinweis: Soweit auf einer Webseite Cookies eingesetzt werden, die nicht nur für die Funktion der Webseite notwendig sind, muss also jeweils eine Einwilligung beim Nutzer eingeholt werden. „Nicht notwendige Cookies“ werden zum Beispiel genutzt für ein Tracking, zu statistischen Zwecken, für Werbung oder den Zugriff externer Medien. Die Einwilligung darf für diese nicht voreingestellt sein. Außerdem muss darauf hingewiesen werden, dass die Einwilligungen jederzeit widerrufen bzw. geändert werden können. Die Datenschutzinformation muss einen entsprechenden Hinweis enthalten.

Im Ergebnis sollten die Unternehmen, die noch immer auf ihren Webseiten ein sog. „Opt-Out-Verfahren“ einsetzen, ihr Cookie-Banner austauschen, auf den aktuellen Stand bringen sowie die Informationen zu deren Verwendung entsprechend den Grundsätzen des BGH bzw. EuGH anpassen. Wenn Sie hierzu Unterstützung benötigen, sprechen Sie Ihren Berater der mip an.

Datenschutzerklärung – ein unpräziser Begriff?

In Art. 13 und 14 DSGVO sind die datenschutz-rechtlichen Informationspflichten geregelt. Unternehmen haben daher insbesondere entsprechende Texte auf ihren Webseiten eingestellt, in denen Nutzer z.B. über den Umfang, Zweck und Art der Datenverarbeitung informiert werden. Diese Informationen sind häufig mit dem Begriff „Datenschutz**erklärung**“ überschrieben. Unter den

Datenschützern ist nun vor dem Hintergrund einer aktuellen Gerichtsentscheidung die Diskussion entbrannt, ob der Begriff Datenschutzerklärung zutreffend ist. Tatsächlich wird hier **keine** Erklärung des Betroffenen abgegeben. Vielmehr wird er **informiert**. Daher sollte der Begriff „**Datenschutzinformation**“ verwendet werden. In der besagten Gerichtsentscheidung hatte das Gericht nämlich damit argumentiert, dass Informationen in der Datenschutzinformation zu vertraglichen Pflichten geworden seien, weil diese mit dem Wort „Datenschutzerklärung“ überschrieben worden war.

Praxishinweis: Überprüfen Sie Ihre Templates, Musterdokumente und Webseiten und passen Sie diese an. Gerne unterstütze wir Sie mit Hilfen und Checks!

Impressum

mip Consult GmbH
Wilhelm-Kabus-Straße 9
10829 Berlin
Tel: +49 (0) 30 – 20 88 999 – 00
Fax: +49 (0) 30 – 20 88 999 – 88
Redaktion: Stefan Ax, Yanick Röhricht, Asmus Eggert

Internet: www.sofortdatenschutz.de und www.blog.sofortdatenschutz.de
E-Mail: sofortdatenschutz@mip-consult.de

Vertretungsberechtigte Geschäftsführer: Asmus Eggert, Uwe Leider
Registergericht: Amtsgericht Berlin-Charlottenburg
Registernummer: HRB 121869
USt.-Identnr.: DE249276018
Verantwortlich nach § 55 Abs. 2 RStV: Asmus Eggert