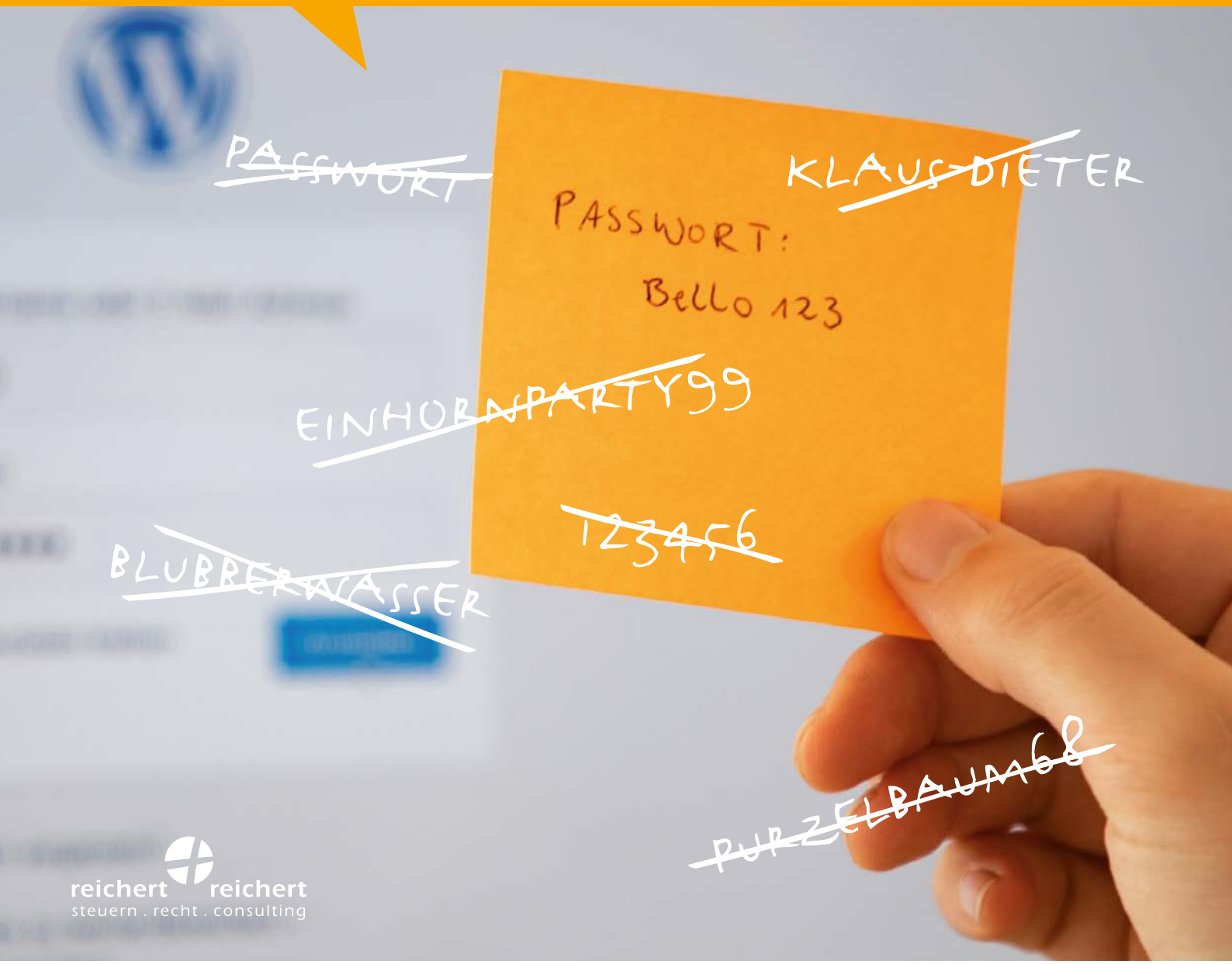
Fokus **DATENSCHUTZ** | **2**

Der **Querdenker**

Themen aus der Kanzlei **reichert & reichert**



reichert reichert
steuern . recht . consulting

DER ZWEITE QUERDENKER
zum Thema Datenschutz

Ist das Thema Datenschutz jetzt durch? Es wäre fatal dies zu glauben, auch in unserem eigenen Interesse. Nein so ist es nicht, vielmehr beginnen die Datenschutzbehörden inzwischen von der eher beratenden Tätigkeit zu zum Teil deutlichen Bußgeldern überzugehen.
In vielen Unternehmen ist das Thema angekommen. Und es bringt auch klare Vorteile, z.B. bei Datenpannen (z.B. Email an den falschen Empfänger). Es ist ja durchaus wichtig, dass solche Informationen mittlerweile in die Chefetage gelangen und nicht „niederschwellig" erledigt werden.

IT-gestützte Prozesse sind heute in unserem Betriebsalltag Normalität geworden. Beginnend bei Handwerksbetrieben, die ihre Angebote per E-Mail versenden oder auf Baustellen digitale Fotografien anfertigen, über mittelständische Unternehmen, die oft ihr gesamtes Kunden- und Lieferantenmanagement in CRM-Systemen abbilden bis zu KI-Systemen in Klinken und in der Pflege – die Digitalisierung ist Teil unserer Arbeitswelt. Als Unternehmer stehen wir vor der Aufgabe, diese Entwicklungen zu nutzen und von ihnen zu profitieren. Dies kann nur gelingen, wenn wir uns aktiv mit Fragen der Datensicherheit und des Datenschutzes auseinandersetzen.

Mit unserem neuen Querdenker Datenschutz II geben wir Ihnen Denkanstöße und würden uns freuen, mit Ihnen ins Gespräch zu kommen.

Und wenn Sie wissen wollen wo Ihr Unternehmen in der Umsetzung der Anforderungen der DSGVO steht, nutzen Sie gerne unseren Quickcheck. Wir sprechen vor Ort mit Ihnen den Stand der Datenschutzthemen durch und erstellen Ihnen einen Fahrplan, in welchen Themenkomplexen noch Handlungsbedarf besteht. Und natürlich unterstützen und beraten wir Sie auch gerne ganz praktisch bei der anschließenden Umsetzung notwendiger Maßnahmen.

Herzlichst, Ihr Dr. Hansjörg Reichert

Datenschutz, Datensicherheit und immer neue Herausforderungen

Nachdem die zahlreichen Unsicherheiten und die, in den Worten des Bundesbeauftragten für den Datenschutz und die Informationssicherheit »teils absurde Panikmache« und »mitunter abwegigen Diskussionen« zum Anwendungsbeginn der Europäischen Datenschutzgrundverordnung (DSGVO) überstanden sind, richtet sich der Blick in der Praxis zunehmend auf den praktischen und alltäglichen Vollzug datenschutzrechtlicher Vorschriften. Spätestens hierbei zeigt sich, ob sich die bis dahin umgesetzten Maßnahmen tatsächlich bewähren und zu mehr Datenschutz und Datensicherheit im Unternehmen führen, oder ob theoretische und standardisierte Datenschutzlösungen »von der Stange« nur dazu dienen, einen als regulatorisch und belastend empfundenen gesetzlichen Anforderungskatalog zu erfüllen.

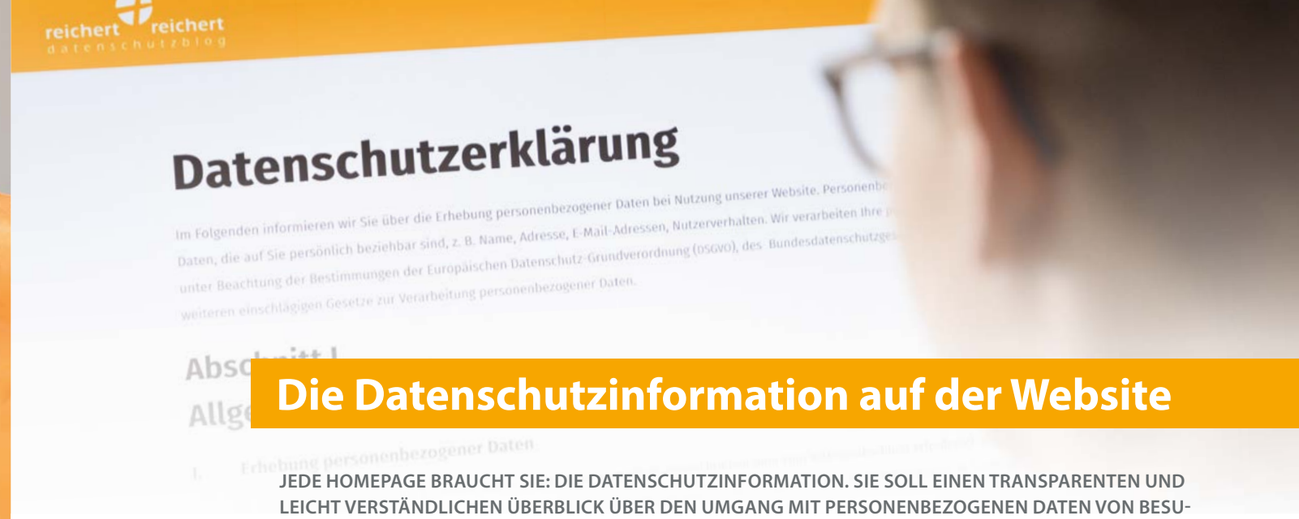
In diesem Kontext hat sich auch der Anspruch an datenschutzrechtliche Konzepte und an die gesetzlich definierte beratende und überwachende Aufgabe der Datenschutzbeauftragten verändert. Datenschutz ist (und war es auch früher) keine »Insellösung« sondern Teil eines modernen Sicherheitskonzeptes, das neben rechtlichen Themen auch umfangreiche und moderne IT-Sicherheitslösungen unterstützt.

Vor diesem Hintergrund bieten wir Ihnen mit unserer vorliegenden Querdenker-Broschüre »Datenschutz II« diesmal mit Blick auf digitale Anwendungen und Prozesse eine Themenauswahl an der Schnittstelle von Datenschutz und Datensicherheit.

Und weil die schnelle Entwicklung im Datenschutz sich zunehmend dem Medium »Broschüre« entzieht, laden wir Sie ein, sich auch auf unserem Blog umzusehen. Unter www.datenschutz-am-bodensee.com bloggt unser Team wöchentlich Themen rund um den Datenschutz, kommentiert Nachrichten der Aufsichtsbehörden und anderer Portale und veröffentlicht viele praktische Hinweise und Umsetzungsempfehlungen aus unserer Beratungspraxis.

IHR ANSPRECHPARTNER:

MATTHIAS HERKERT,
LEITER CONSULTING



Die Datenschutzinformation auf der Website

JEDE HOMEPAGE BRAUCHT SIE: DIE DATENSCHUTZINFORMATION. SIE SOLL EINEN TRANSPARENTEN UND LEICHT VERSTÄNDLICHEN ÜBERBLICK ÜBER DEN UMGANG MIT PERSONENBEZOGENEN DATEN VON BESUCHERN UND NUTZERN DER WEBSITE GEBEN. BEI DER ERSTELLUNG DER DATENSCHUTZINFORMATION IST DAMIT IMMER AUCH EIN BLICK INS DETAIL WICHTIG, DENN ES KOMMT NICHT NUR DARAUF AN, DEN NUTZER ÜBER SOLCHE VERARBEITUNGEN ZU INFORMIEREN, AN DENEN ER AKTIV BETEILIGT IST (Z.B. ERHEBUNG VON DATEN ÜBER EIN KONTAKTFORMULAR ODER ANMELDUNG IN EINEM SHOPMODUL), SONDERN AUCH ÜBER SOLCHE, DIE AUSSERHALB DER WAHRNEHMUNG LIEGEN.

Verantwortlicher und Datenschutzbeauftragter

Meistens sind an der Erstellung einer Website mehrere Personen oder Unternehmen beteiligt. Die Website ist powered by, Programmierung und Design stammen aus verschiedenen Federn, die inhaltliche Verantwortlichkeit liegt bei einem im Unternehmen Beschäftigten und der im Drittland sitzende Mutterkonzern hat die Betreuung der Website an die deutsche Tochter abgegeben.

Die Datenschutzinformation muss dabei angeben, wer für die Datenverarbeitungen auf der Website verantwortlich (!) ist. Diese Frage lässt sich allerdings nicht nur bei großen Plattformbetreibern wie Facebook oder Instagram schwer beantworten. Entscheidend ist nicht, wer die Website betreut. Die Frage, wer Eigentümer der personenbezogenen Daten ist, kann hier oft weiterhelfen. Ziehen Sie dafür Ihren Datenschutzbeauftragten hinzu. Übrigens gehören auch dessen Kontaktdaten in die Datenschutzerklärung.

Log-Files

Tückisch! Seitdem der EuGH IP-Adressen einen Personenbezug zugeordnet hat, hat in fast allen Fällen allein der Aufruf einer Website zur Folge, dass personenbezogene Daten übermittelt werden. Die in Log-Files gespeicherten Daten müssen daher in der Datenschutzinformation aufgelistet werden. Fragen Sie Ihren Host oder Programmierer, er kann Ihnen weiterhelfen.

Cookies

Ein nicht zu unterschätzender Regelungspunkt sind Cookies. Aufgrund der hohen Werberelevanz und der Möglichkeit, über Cookies ganze Nutzerprofile anzulegen, ist bei der Transparenz besondere Sorgfalt geboten. Lassen Sie sich auch hier von Ihrem Programmierer helfen und ein Cookie-Verzeichnis geben, das Informationen über den Namen, den Anbieter, den Zweck und die Laufzeit eines jeden Cookies beinhaltet.

Werden mit Cookies die Verhalten von Nutzern getrackt oder personalisierte Werbung im Rahmen des Online-Marketings ausgespielt, muss zuvor eine Einwilligung der Nutzer eingeholt werden (vgl. Beitrag Einwilligungen im Online-Marketing).

Einbindung von Inhalten Dritter

Webservices und Plug-Ins, die von Dritten angeboten werden und vom Verantwortlichen in der Website integriert sind, sind ebenfalls in der Datenschutzinformation anzugeben. Der Dritte sollte hierbei immer benannt werden, da auch an ihn Daten übermittelt werden, auf die der Verantwortliche keinen Einfluss mehr hat. Dem Nutzer muss daher eine Möglichkeit geboten werden, seine Rechte beim betreffenden Dritten geltend machen zu können. Inhalte Dritter sind z.B. Social Media Plug-Ins von Facebook oder Twitter oder APIs, über die Daten und Inhalte zwischen verschiedenen Webseiten ausgetauscht werden können.

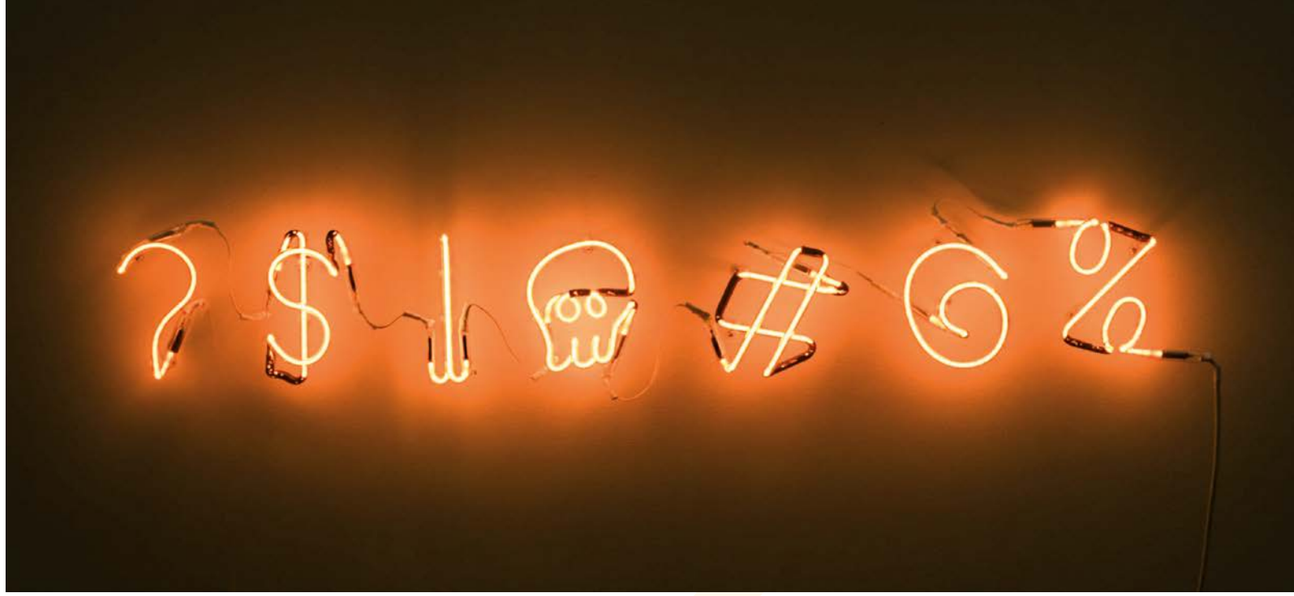
Die oben benannten Punkte bilden nur eine kleine Auswahl an Verarbeitungen ab, die in der Datenschutzinformation anzugeben sind. Art. 13, 14 DSGVO sehen daneben weitere Angaben vor. Achten Sie darauf, auch hinter die Website zu schauen und den Weg von IP-Adressen zu verfolgen.

IHRE ANSPRECHPARTNERIN:

EILEEN BINDER,
WIRTSCHAFTSJURISTIN

PASSWORTSICHERHEIT
als Pflicht im Datenschutz

DER LANDESDATENSCHUTZBEAUFTRAGTE IN BADEN-WÜRTTEMBERG (LFDI BW) HAT BEREITS MITTE FEBRUAR 2019 HINWEISE ZUM UMGANG MIT PASSWÖRTERN UND ZUR PASSWORTSICHERHEIT VERÖFFENTLICHT. DIE HINWEISE GEBEN IN IHRER ÜBERSICHT EINE WERTVOLLE „CHECKLISTE" ZUR IT-SICHERHEIT UND ZUR UMSETZUNG DER DATENSCHUTZRECHTLICHEN SICHERHEITSANFORDERUNGEN.



Von starken Passwörtern, Lügen und dem Konflikt zwischen Passwortlänge und Displaygröße – Passwortsicherheit für Anwender

Vor dem Hintergrund, dass die Anmeldung zur Nutzung von IT-Devices und IT-Strukturen mittels Nutznamen und Passwort nach wie vor das gängigste Verfahren zur Authentifizierung darstellt, gibt der Landesdatenschutzbeauftragte zehn Empfehlungen zur Auswahl „sicherer" Passwörter und zum Passwortmanagement für Privatpersonen. Dabei führt er „alte Bekannte" wie die Empfehlung für starke Passworte (d.h. lange Passworte mit Klein- und Großbuchstaben, Ziffern und Satzzeichen) an, die mit Aussagen wie „je wichtiger das Passwort ist, desto länger sollte es sein" kaum überraschen und schlägt einmal mehr „Systeme" zur Entwicklung und Memorierung von Passwörtern wie die „Ganze-Satz-Methode" und die „erster-Buchstaben-Methode" vor. Zusammen mit der Empfehlung keine Wörter aus Wörterbüchern zu verwenden, sichere Passwörter auch auf Smartphones einzusetzen, Passwörter nicht weiterzugeben und voreingestellte Standard-Passwörter bei der ersten Verwendung des Dienstes / Systems sofort zu ändern, erscheint der Empfehlungskatalog an einigen Stellen zum einen beinahe „überraschend pauschal", erschreckend zum anderen, dass solche Empfehlungen auch heute noch sinnvoll und notwendig sind.

Durchdacht und im Schlaglicht des Datenschutzes gleich in mehrfacher Sicht sinnvoll, erscheint indes die Empfehlung zur „Lüge bei Sicherheitsfragen". Hier rät der Landesbeauftragte dazu, bei Sicherheitsfragen von Diensten, die nach persönlichen Informationen als Antwort fragen („Wohin sind Sie zum ersten mal in Urlaub geflogen" oder „Wie war der Name Ihres besten Freundes in der Grundschule") zur bewussten Lüge. Zum einen wird hierdurch verhindert, dass Angreifer aus dem Umfeld des Passwortverwenders dieses erraten können, zum anderen finden Informationen nicht über „Umwege" den Weg z.B. ins Internet.

Kritisch bleibt freilich die Frage, ob man sich zum gegebenen Zeitpunkt noch an seine bewusste Lüge erinnern kann – aber dieses Problem ist jeder Lüge immanent.

Weiter bricht der Landesbeauftragte mit seiner Empfehlung, Passwörter nur bei einem Verdacht der Kompromittierung zu ändern, mit der langjährigen Empfehlungspraxis vieler IT-Sicherheitsexperten, Passwörter in regelmäßigen Abständen zu erneuern. So sinnvoll diese Empfehlung jedoch gegenüber fachlich qualifizierten Nutzern sein mag, so problematisch kann es sein, die „Entscheidung" über eine möglich Kompromittierung im betrieblichen Alltag auf den Anwender zu verlagern.

Vom notwendigen Zusammenspiel vieler Maßnahmen, dem Stand der Technik und der Verantwortung der Geschäftsführung – Passwortsicherheit im Unternehmen

Deutlich präziser und Richtungsweisender wird der Landesdatenschutzbeauftragte BW bei seinen „Hinweisen für Administratoren und Entwickler", die insbesondere für IT-Verantwortliche, aber gerade auch für Geschäftsführer und Vorstände von Unternehmen und Vereinen, die sich in ihrer täglichen Arbeit nicht regelmäßig mit den Themen der Passwortsicherheit und Kryptografie beschäftigen, einen guten Überblick über den „Stand der Technik" im Bereich der Passwortsicherheit geben.

Zum Einstieg baut der LfDI BW eine Brücke zu den Empfehlungen der Anwender, indem er rät, die dort gegebenen Hinweise in eine Passwort-Richtlinie einzubinden.

Mit der Übertragung des Hinweises, die früher vertretene regelmäßige Änderung von Passwörtern durch eine wirksame Sensibilisierung der Beschäftigten zu ersetzen, folgt der LfDi BW den Empfehlung des National Cyber Security Centre wie auch des National Institute of Standards and Technology des U.S. Department of Commerce.

Über einen Hinweis auf mögliche Verstöße gegen Art. 32 DSGVO wie auch die hierzu bereits verhängten Geldbußen wird auf die Notwendigkeit der Nutzung moderner Passwort-Hashing-Verfahren und die Sicherstellung ausreichender Entropie hingewiesen.

Ebenfalls in die Blickrichtung der Passwortspeicherung geht die Empfehlung, Passwort-Datenbanken besonders zu sichern und auch auf der Ebene der Administratoren eine restriktive Rechte- und Rollenstruktur anzuwenden. Interessanterweise verzichtet der LfDi BW hierbei, anders als zuvor, auf einen Verweis auf Art. 32 DSGVO.

Die Forderung „soweit möglich" immer Zwei-Faktor-Authentifizierungen zu implementieren kombiniert der Landesdatenschutzbeauftragte mit dem Hinweis, den Benutzer hierbei nicht durch die Hintertüre zur Preisgabe bislang nicht erhobener personenbezogener Daten, im Beispiel zur Herausgabe einer Mobilfunknummer, zu nötigen und greift hier, ohne ausdrückliche Erwähnung, den Grundsatz der Datenminimierung auf.

Die Anforderung an Administratoren und Entwickler, bei Inbetriebnahme eines Gerätes oder Dienstes die Änderung voreingestellter Passwörter zu erzwingen, schließt an die Empfehlung gegenüber Anwendern an, Standard-Passwörter immer zu ersetzen.

Da erfolglose Anmeldeversuche in der Praxis auf interne oder externe Angriffe (Eindringversuche) hinweisen können, sollten fehlgeschlagene Anmeldeversuche protokolliert und regelmäßig analysiert werden. Und auch wenn dies nicht erwähnt wird, ist jeder Verantwortliche gut beraten, das Auslesen dieser Protokolle zu „üben", damit im Bedarfsfall keine zeitintensiven Abstimmungen mit der IT-Abteilung oder Administratoren erforderlich sind.

Mit der abschließenden Empfehlung an Online-Dienstanbieter, grundsätzlich keine fremden Passwörter zu sammeln und bei Bedarf standardisierte, sichere API-Autorisierungen und Frameworks zum Austausch von Authentifizierungs- und Autorisierungsinformationen zu nutzen, fokussiert die Handreichung nochmals direkt auf die Anforderungen an die Sicherheit der Verarbeitung aus Art. 32 DSGVO.

Fazit

Im Ergebnis bringen die Empfehlungen für Privatanwender kaum Neues, fassen jedoch den Stand der Diskussion zur Passwortsicherheit mit Blickrichtung auf den privaten wie betrieblichen User nochmals gut zusammen.

Die Hinweise an Administratoren und Entwickler, die ohne weiteres als Hinweise an Geschäftsführer und Verantwortliche verstanden werden sollten, gehen indes deutlich intensiver auf die wohl als „Stand der Technik" zu wertenden Möglichkeiten der Sicherheit der Verarbeitung ein. Die Empfehlungen verdeutlichen zum einen die bereits heute umfangreichen Möglichkeiten zur Gestaltung starker Passwörter und zu einer entsprechenden Passwortsicherheit, zum anderen aber auch die Notwendigkeit zur Umsetzung dieser Themen in der Praxis. Verantwortliche können sich heute keinesfalls mehr auf „technische Unwissenheit" oder eine „praktische Übung der gesamten Branche" berufen.

IHR ANSPRECHPARTNER:

MATTHIAS HERKERT,
LEITER CONSULTING

Unsichere Datenübertragung

BEI VERWENDUNG VON SSL-PROTOKOLLEN

DAS BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI) HAT DAS ZU FORDERNDE MINDESTNIVEAU FÜR DIE INFORMATIONSSICHERHEIT BEI DER ÜBERTRAGUNG VON INFORMATIONEN ÜBER KOMMUNIKATIONS- UND DATENNETZE ANGEHOBEN UND SEINE EMPFEHLUNGEN FÜR DEN EINSATZ DES KRYPTOGRAPHISCHEN TLS-PROTOKOLLS AKTUALISIERT. FÜR VIELE UNTERNEHMEN BESTEHT NUN HANDLUNGSBEDARF.

Durch den Einsatz der seit Anfang April 2019 vom BSI empfohlenen Protokolle wird bei der Datenübertragung zwischen den beiden Verbindungspartnern ein verschlüsselter, authentisierter und integritätsgeschützter Kanal aufgebaut, der eine sichere Übertragung der Informationen über TCP/IP-basierte Verbindungen ermöglicht. In ihrer „Technischen Richtlinie TR-02102–2 zum Einsatz von kryptographischen Verfahren" werden hierzu die SSL-Protokolle (Secure Sockets Layer) SSL v2 und SSL v3 genauso wie die TLS-Versionen (Transport Layer Security) 1.0 und 1.1 als nicht mehr ausreichend sicher eingestuft. Empfohlen wird der Einsatz der Verschlüsselungsprotokolle TLS 1.2 und TLS 1.3, jeweils in Kombination mit Perfect Forward Secrecy (PFS).

Der Einsatz von TLS-Versionen die älter als TLS 1.2 sind wird von der nationale Cyber-Sicherheitsbehörde in der „Stellungnahme zu Mindeststandards des BSI zur Verwendung von Transport Layer Security (TLS)" hierbei ausdrücklich als „ein Risiko für die Informationssicherheit" bezeichnet.

Empfehlungscharakter und Verbindlichkeit der Mindestanforderungen

Mit den vorliegenden Mindeststandards erfüllt das Bundesamt für Sicherheit in der Informationstechnik seinen gesetzlichen Auftrag gemäß § 8 Abs.1 S. 1 BSIG. Das Bundesministerium des Innern kann diese Mindeststandards ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes einsetzen. Auch wenn die Mindeststandards zur Informationssicherheit bei der Datenübertragung damit weder in den Behörden des Bundes oder der Länder, noch in der freien Wirtschaft unmittelbar verbindlich sind, stellen die Empfehlungen sehr konkrete Mindestniveaus dar, die auch von den Aufsichtsbehörden ganz regelmäßig als Stand der Technik unter anderem im Kontext des Artikel 32 DSGVO interpretiert werden.

Auch der Einsatz des Transport Layer Security (TLS) Protokolls bietet keine abschließende Übertragungssicherheit

Das BSI weist zudem ausdrücklich auch auf die verbleibenden Risiken hin, die beim Einsatz des kryptographischen TLS-Protokolls fortbestehen. Da auch das TLS-Protokoll Verbindungen zulässt, die nur einseitig (i.d.R. auf Serverseite) authentisiert sind, werden die Entwickler kryptographischer Systeme aufgefordert, bei der Risikobeurteilung grundsätzlich zu prüfen, ob weitere Authentisierungen, zum Beispiel durch den Einsatz der Zwei-Faktor-Authentisierung, erforderlich sind.

Konkreter Handlungsbedarf

Unternehmen und Behörden, die bei der Datenübertragung noch SSL v2, SSL v3 oder TLS 1.0 bzw. TLS 1.1 Protokolle verwenden, sollten diese kurzfristig identifizieren und an die Mindeststandards anheben, um ihre Datenübertragung kryptographisch abzusichern. Argumente wie die Anforderung der Anwender an die Abwärtskompatibilität können mit Blick auf die Risiken für die Inormationssicherheit keinesfalls zur Unterschreitung des „Stands der Technik" herangezogen werden.

Bei der Planung und späteren Umsetzung der Maßnahmen sollten die Verantwortlichen unbedingt neben internem oder externem IT-Sicherheits-Know-How immer auch den Datenschutz mit hinzuziehen, damit neben den möglicherweise notwenigen rechtlichen Einschätzungen auch die Erfüllung der gesetzlichen Nachweispflichten aus Artikel 5 Abs. 2 DSGVO gewährleiste ist.

IHR ANSPRECHPARTNER:

MATTHIAS HERKERT,
LEITER CONSULTING

Einwilligungen im ONLINEMARKETING

E-MAILMARKETING IST IMMER NOCH EINES DER BELIEBTESTEN MITTEL, UM IM DIGITALEN BEREICH MIT DEM ENDVERBRAUCHER IN KONTAKT ZU TRETEN. GLEICHZEITIG IST E-MAILMARKETING ABER AUCH EIN MIT VIELEN STOLPERFALLEN VERBUNDENES MITTEL. BEVOR DER VERANTWORTLICHE MIT DEM WERBEEMPFÄNGER IN KONTAKT TRITT, SOLLTE DAHER GENAU GEPRÜFT WERDEN, UNTER WELCHEN BEDINGUNGEN DER „ELEKTRONISCHE BRIEF" ZULÄSSIG IST. DENN UNZULÄSSIGE E-MAILWERBUNG IST BUSSGELDBEDROHT!

Der sicherste Weg für die zulässige Versendung von E-Mailwerbung ist nach wie vor die vorherige Einwilligung den Empfängers (Art. 6 Abs. 1 S. 1 lit. a DSGVO).

Die Voraussetzungen einer datenschutzkonformen Einwilligung sind schnell zusammengefasst: Sie muss präzise, transparent und verständlich formuliert sein und darüber informieren, wer zu welchem Zweck wie oft Werbung versendet und ob ggf. Dritte beteiligt sind. Der Werbeempfänger muss die Einwilligung freiwillig abgeben und die Möglichkeit haben, seine Willensäußerung jederzeit zu widerrufen.

IM EINZELNEN BEDEUTET DAS...

Zweck

Die Einwilligungserklärung muss darüber informieren, dass die erhobenen Daten zum Zwecke der Direktwerbung (!) verarbeitet werden. Dabei sollte die Zweckbeschreibung auch Informationen darüber enthalten, wie oft Werbung versendet wird und um welche Form von Werbung es sich handelt. Der Begriff Werbung ist hierbei weit auszulegen und umfasst u.a. Newsletter, Aktions- und Rabattangebote, Produktwerbung, Trigger-Mailings und selbst Veranstaltungseinladungen und Mailings mit Weihnachtsgrüßen gehören dazu.

Freiwilligkeit

Die Einwilligung muss freiwillig abgegeben werden. Eine Freiwilligkeit ist insbesondere dann nicht anzunehmen, wenn die Erfüllung eines Vertrages oder die Erbringung einer Dienstleistung von der Einwilligung abhängt (Koppelungsverbot). So stellt beispielsweise die Teilnahme an einem Gewinnspiel unter der Bedingung, kostenlos Werbung zusenden zu dürfen, regelmäßig keine entkoppelte Willensäußerung dar.

Dritte

Wird z.B. für den E-Mailversand ein Versanddienstleister genutzt, ist der Einwilligende auch dar-über zu informieren, dass seine Daten an diesen Dritten weitergegeben werden. Das ist insbesondere dann notwendig, wenn der Dienstleister weder im Inland noch in der EU oder dem EWR sitzt.

Widerruf

Wichtig ist zudem, den Werbeempfänger darüber aufzuklären, dass er seine Einwilligung jeder-zeit widerrufen kann. Der Hinweis muss zwingend vor Abgabe der Einwilligungserklärung erfolgt sein. Zudem muss der Widerruf so einfach abzugeben sein wie die Einwilligung selber. Ein Link zur Abbestellung der Werbung in jeder E-Mail genügt den Anforderungen.

WAS IST NOCH ZU BEACHTEN?

Die Voraussetzungen müssen bei der Erteilung der Einwilligung erfüllt sein und alle notwendigen Informationen müssen zum Zeitpunkt der Erhebung mitgeteilt werden. Die personenbezogenen Daten, die der Verantwortliche beim Werbeempfänger erhebt, müssen sich auf die Daten beschränken, die für die Erbringung seiner Leistung unbedingt erforder-lich sind. Wer Werbung ausschließlich per E-Mail versendet, kann z.B. auf die Postadresse des Empfängers oder dessen Mobilfunknummer verzichten. Außerdem muss der Verantwortliche neben der Gewährleistung angemessener Datensicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten für das Onlinemarketing stets beachten, dass die DSGVO umfassende Rechenschaftspflichten auferlegt. Er muss daher nachweisen können, dass die betroffene Person in den Erhalt von Werbung eingewilligt hat. Für das elektronische Erklären einer Einwilligung bietet sich das Double Opt-In-Verfahren an. Für den Nachweis genügt die Protokollierung des Double Opt-In-Verfahrens sowie des Inhalts der Einwilligung.

IHRE ANSPRECHPARTNERIN:

EILEEN BINDER,
WIRTSCHAFTSJURISTIN

Videoüberwachung
durch nicht öffentliche Stellen

SEI ES DER EINSATZ VON KAMERAS AN PRIVATHÄUSERN, DIE ÜBERWACHUNG VON MITARBEITERN IN VERKAUFSRÄUMEN, KAMERAS IN DER GASTRONOMIE ODER DER EINSATZ SONSTIGER KAMERASYSTEME WIE WEBCAMS, DASHCAMS UND DROHNEN – DIE EINSATZGEBIETE KAMERAGESTÜTZTER ÜBERWACHUNGSMASSNAHMEN SIND VIELFÄLTIG UND NEHMEN RASANT ZU.

Mit Einführung der DSGVO haben die Diskussionen über den Einsatz von Videokameras wieder an Fahrt aufgenommen. Sowohl für die Aufsichtsbehörden als auch für Betreiber von Videoüberwachungssystemen ist das Thema von erheblicher praktischer Relevanz.

Neben der Erfüllung der individuellen Informationspflichten gegenüber den von den Aufzeichnungen betroffenen Personen und der gerade in diesen Fällen wichtigen Planung der technischen Sicherheit der Systeme und Aufzeichnungen, ist insbesondere die Rechtsgrundlage für den Betrieb des Videosystems von besonderer Bedeutung.

Wann ist der Betrieb einer Videoüberwachungsanlage rechtmäßig

Beim Einsatz eines Videoüberwachungssystems handelt es sich zweifelsohne um eine Datenverarbeitung im Sinne der DSGVO, weshalb die Vorschriften über den Datenschutz regelmäßig Anwendung finden.

Lediglich Kamerasysteme, die ausschließlich persönlichen oder familiären Tätigkeiten dienen, sind über das „Haushaltsprivileg" gemäß Art. 2 Abs. 2 lit. b DSGVO vom Anwendungsbereich der DSGVO ausgeschlossen. Für alle anderen Tätigkeiten, meist im beruflichen und wirtschaftlichen Bereich, gilt, dass der Einsatz der Videoüberwachungsmaßnahme einen der Rechtsgründe aus Art. 6 DSGVO erfordert. In Betracht kommen neben dem „berechtigten Interesse" die „Einwilligung" und die „Erfüllung einer rechtlichen Verpflichtung".

Einwilligung

Die Rechtsmäßigkeit der Videoüberwachung auf eine Einwilligung der betroffenen Personen im Sinne des Art. 6 Abs. 1 S. 1 lit. a DSGVO zu stützen, wird in der Praxis in den meisten Fällen kaum möglich sein. Und auch die Annahme einer konkludenten Einwilligung würde hier zu weit gehen, da z.B. das Betreten eines videoüberwachten Bereichs nicht als eindeutig bestätigende Handlung zu werten sein wird.

Rechtliche Verpflichtung

Auch eine rechtliche Verpflichtung im Sinne des Art. 6 Abs. 1 S. 1 lit. c DSGVO über die eine Videoüberwachung rechtmäßig wäre, wie sie etwa im Kassenbereich von Banken gegeben ist, wird nur in wenigen Ausnahmefällen vorliegen.

Berechtigtes Interesse

Für die Prüfung der Rechtmäßigkeit der Videoüberwachung bleibt somit nur noch die „Generalklausel" aus Art. 6 Abs. 1 S. 1 lit. f DSGVO. Die Datenverarbeitung ist dann rechtmäßig, wenn ein berechtigtes Interesse des Verantwortlichen oder eines Dritten vorliegt, die Verarbeitung erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person(en) nicht überwiegen.

Für die Praxis gilt in diesen Fällen: Bei der Installation einer Videoüberwachungsmaßnahme reicht es nicht aus, sich bloß abstrakt auf ein berechtigtes Interesse zu stützen. Erst die Abwägung im konkreten Einzelfall, sowohl im Hinblick auf die Interessen der Verantwortlichen als auch der betroffenen Personen, kann die Legitimation der Videoüberwachung gegebenenfalls begründen.

Welche Punkte bei einer Abwägung zu berücksichtigen sind, lesen Sie in unserem NEWS-Beitrag „Die Videoüberwachung durch nicht öffentliche Stellen" auf unserem Datenschutzblog **www.datenschutz-am-bodensee.com.**

IHR ANSPRECHPARTNER:

MARKUS SPÖHR,
WIRTSCHAFTSJURIST

TIPP!

Sie möchten den Querdenker weiterempfehlen?
Jetzt online nachlesen:
www.reichert-reichert.de

IMPRESSUM

Herausgeber
reichert & reichert
steuerberater & rechtsanwaltskanzlei
Zeppelinstraße 7 - 78224 Singen
+49 (0) 7731.9587-0
Reichenaustraße 19a - 78467 Konstanz
+49 (0) 7531.81987-0
kanzlei@reichert-reichert.de

erschienen im November 2019
Redaktion
Dr. Hansjörg Reichert, Matthias Herkert, Eileen Binder, Markus Spöhr

Layout & Fotografie
FRANK.COMMUNICATION.
www.frank-com.de