Dezember 2020 | Zum Datenschutz aufgefallen

Information zum

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in),*

Aufsichtsbehörden sind im verpflichtendem Auf – und Ausbau, Verantwortliche wie Privatpersonen und auch Gerichte „*gewöhnen*“ sich langsam an die Pflichten und Rechte aus der EU – DS - GVO. Damit nehmen Neuigkeiten zum Datenschutz nicht ab. Hier finden sich die mir zum Datenschutz aktuell aufgefallenen Nachrichten.

Unter „Inhalt“ sind die Nachrichten übersichtlich aufgeführt. Mit einem Klick gelangen Sie zu einer kurzen Zusammenfassung mit Angabe der Quelle und Link. Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist.

Selbstverständlich können Sie sich auch bei diesen, wie bei allen Fragen zum Datenschutz gerne direkt an mich wenden. Schreiben Sie mir einfach!

Vielen Dank für Interesse

Inhalt

(zusammengestellt von Volker Schroer, zertifizierter Datenschutzbeauftragter)

(1) „SDM“ das Standard – Datenschutz - Modell.....1

(a) Fertig hier Vers. 2.0b.....1

(b) Fertig? Na ja, fast!.....1

(2) Zu Datenschutz.....1

(a) BREXIT – DSGVO Jahresknaller anderer Art.....1

(3) Zu Datensicherheit.....2

(a) Erkenntnisse aus schweren Hacker – Angriffen ?.....2

i) Veröffentlichte Angriffe im Dezember (3 Beispiele):.....2

ii) Wer sind potentielle Angriffsopfer?.....2

iii) Wie erfolgt Auswahl und Angriff?.....2

iv) Wo gibt es Hilfe?.....3

v) Wie kann ich vorgehen?.....3

(4) Zu angrenzenden Themen.....3

(a) Die ganz große *N*ummer!....3

(b) Es geht auch *ganz* anders. .3

(1) „SDM“ das Standard – Datenschutz - Modell

(a) Fertig hier Vers. 2.0b

LINK zum aktuellen Standard – Datenschutz – Modell auf der Seite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit	***PDF 72 Seiten***	SDM Quelle: Link im Bild
LINK zum Standard – Datenschutz in meiner Kurzversion für eilige Leser.	***PDF 9 Seiten***	

(b) Fertig? Na ja, fast!

Da war noch der unvollständige Referenzkatalog, welcher Vorschläge zu Maßnahmen bei hohem Schutzbedarf enthalten soll. Allerdings ist dieser noch nicht vollständig, sondern es liegen nur einzelne Bausteine vor. Ein Liste mit Links (Stand: 12/2020) ist in der Zusammenfassung unter D.4 auf Seite 8 aufgeführt. Bei neuen oder geänderten Bausteinen wird die Liste entsprechend angepasst. Neuerungen oder Änderung werde ich an dieser Stelle mitteilen.

(2) Zu Datenschutz

(a) BREXIT – DSGVO Jahresknaller anderer Art

Wie hörte ich vor kurzer Zeit: „Das war doch klar, alle haben doch bereits reagiert!“ Anm.: „Nee is’ klar, es gab ja kaum andere wichtige Themen in letzter Zeit“ 😐

Mit dem Austritt Großbritanniens gelten die Regeln für „Drittland“ (Angemessenheitsbeschluss, angemessene Garantien u.s.w.). Die Bundesregierung schreibt dazu am 28.12.2020 (LINK):

Zudem regelt das Abkommen den gegenseitigen Datenaustausch, so zum Beispiel von Fluggastdaten oder Strafregistereinträgen. All dies wird im Einklang mit den Bestimmungen der EU-Datenschutzgrundverordnung (DSGVO) und der Europäischen Menschenrechtskonvention geschehen.

Zum weiteren Vorgehen wird auf branchenspezifischen Maßnahmen der Übergangsseite (LINK) verwiesen, welche aus Mitte des Jahres stammen. Da findet sich dann auch ein Dokument zum

Datenschutz (LINK, 5 Seiten.pdf), was vom 9. Januar 2018 datiert. Das Dokument sieht dann die Regeln für Übermittlung Drittland (DS-GVO Kapitel V) vor, wie Angemessenheitsbeschluss (liegt noch nicht vor), geeignete Garantien (Standard – Vertrag – Klauseln, verbindliche interne Datenschutzbestimmungen, Verhaltensregeln, Zertifizierung) und die Ausnahme nach Art.49 DS-GVO (Einwilligung plus wichtiger Grund, Vertragsverhandlungen u.ä.). Auch die aktuelle Version vom 15.12.2020 des European Data Protection Board (LINK) trifft keine andere Aussage. Es gibt eine Ausnahme nach Artikel 71 des Austrittsabkommen (LINK) der besagt:

Das Unionsrecht über den Schutz personenbezogener Daten gilt im Vereinigten Königreich für die Verarbeitung der personenbezogenen Daten betroffener Personen außerhalb des Vereinigten Königreichs, sofern die personenbezogenen Daten a) vor dem Ablauf des Übergangszeitraums im Vereinigten Königreich gemäß dem Unionsrecht verarbeitet wurden (!) oder b) nach dem Ablauf des Übergangszeitraums aufgrund des vorliegenden Abkommens (*) im Vereinigten Königreich verarbeitet werden.

*) d. h. nach DS-GVO. Solange GB nicht vergleichbare Regelungen verabschiedet gilt auch hier das EuGH – Urteil zu Schrems II (Informationsbrief Juli (LINK) unter 2.a EuGH Entscheidung)

(3) Zu Datensicherheit

(a) Erkenntnisse aus schweren Hacker – Angriffen ?

i) Veröffentlichte Angriffe im Dezember (3 Beispiele):

➔ heise-online: Ransomware - Cyberangriff auf Zeitarbeitsfirma Randstad (LINK)

Auszug: *Sobald dieser Angriff auf die IT-Netzwerke bemerkt wurde, hat das Unternehmen die für solche Fälle vorhandenen Notfallpläne für die IT-Systeme aktiviert. Ein internes Incident Response Team nahm unverzüglich die Arbeit auf und zog externe Cybersicherheits- und Forensik-Experten zur Untersuchung und Behebung des Vorfalls hinzu. Laut Bleeping Computer, hat die Egregor-Ransomware-Gruppe ein 32,7 MB großes Archiv mit 184 Dateien veröffentlicht. Dieses Archiv soll etwa 1 Prozent der erbeuteten Randstad-Daten umfassen und enthält Kalkulationstabellen, Finanzberichte, Verträge und verschiedene andere Geschäftsunterlagen, die durch die Ransomware von den Servern abgezogen und an die Rechner der Cyberkriminellen übermittelt wurden.*

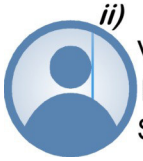
➔ Handelsblatt: Hacker legen Symrise AG lahm – Ransomware vermutet (LINK)

Auszug: *Während die Polizei ermittelt, steht die Produktion des Aromaspezialisten weitgehend still. Um die Folgen bewerten zu können und mögliche weitere Auswirkungen zu verhindern, hat das Unternehmen alle wesentlichen Systeme heruntergefahren", teilte Symrise mit.*

➔ WELT: Die Funke-Erpressung war das „ideale Verbrechen" – Ransomware (LINK)

Auszug: *Kurz vor Weihnachten ist die Funke Mediengruppe Opfer eines schweren Hackerangriffs geworden. Es zeigt sich, warum die Verbrecher keine Strafverfolgung zu fürchten haben – und warum das Ganze noch sehr teuer für Funke werden kann. Zahlt das Opfer, dann liefern die Täter meistens auch den digitalen Schlüssel zur Rettung der Daten. „Die Gruppen achten tatsächlich darauf, dass auf Zahlung auch die Datenrettung folgt, sie richten sogar eine Art Kundenservice ein", berichtet Trost. „Denn wenn das nicht klappt, wäre es schlecht fürs Geschäft." Nach dem Lösegeld fängt für das betroffene Unternehmen die Arbeit aber erst an. Die Systeme wieder einzurichten und sie digital zu säubern, dauert Wochen. In manchen Fällen müssen sogar Teile der Hardware ausgetauscht werden. Nur wenn alles neu aufgesetzt ist, können die IT-Experten sicher sein, dass kein zweiter Angriff folgt. Für Funke wird es also auf jeden Fall noch richtig teuer.*

ii) Wer sind potentielle Angriffsopfer?



Vereinfacht ausgedrückt können alle zum Opfer von Hackerangriffen werden. Unternehmen wie Randstad, Symrise oder Funke sind die lukrativen Opfer. Bei KMU, Gewerbetreibenden, Selbstständigen bis zu Privatpersonen macht es die Menge im Verhältnis zum Aufwand.

iii) Wie erfolgt Auswahl und Angriff?

Das die Cyberkriminalität in Arbeitsteilung Wertschöpfungsketten bildet (CCaaS) zeigt sehr schön und verständlich das Bundeslagebild 2019 des BKA (LINK) auf. Die Auswahl teile ich hier in zwei Hauptmerkmale. 1.) Zufallsprinzip: Durch Massenmails (Spam) werden die „Spione" verteilt und die „Infizierten" ob Unternehmen oder Privatperson nach Potential ausspioniert. 2.) Zielauswahl: Unabhängig von Branche, Position oder Identität haben Hacker vor allem die Mitarbeiter im Visier. Von Interesse sind deren E-Mail-Adressen, Passwörter, Bankkonten, aber auch verschlüsselte Datenbanken. Bei lukrativen Zielobjekten werden Mitarbeiter und Unternehmen zusätzlich über Social – Media und / oder Social – Engineering ausspioniert um einen gezielten Angriff vorzubereiten und erfolgreich durchzuführen.

iv) Wo gibt es Hilfe?

Das Angebot ist natürlich vielfältig, fast unübersichtlich. Nahestehend ist der eigene IT – Service ob Abteilung oder Servicedienstleister. Interessant finde ich die Initiative „NO MORE RANSOME!“, Die Website "No More Ransom" ist eine Initiative der National High Tech Crime Unit der niederländischen Polizei, Europols europäischem Cybercrime Center, Kaspersky und McAfee. Ziel ist es, Opfern von Ransomware bei der Entschlüsselung zu helfen, ohne dass das Lösegeld an die Cyberkriminellen bezahlt wird. Um die Geschäfte von Cyberkriminellen zu stören, haben sich Strafverfolgungsbehörden und IT – Security - Unternehmen zusammengetan. Die Partner – Liste liest sich wie das Who is Who der Strafverfolgungsbehörden und Sicherheitssoftware Unternehmen. Ich denke ein Blick auf die Netzseite lohnt sich: https://www.nomoreransom.org.

v) Wie kann ich vorgehen?

Immer gut ist es über einen Notfallplan (IRP – Incedent Responce Plan) zu verfügen. Ein kleiner Entwurf zum Vorgehen in 10 Punkten:

1) Ruhe bewahren: So schwer es auch fallen mag, Ruhe und Konzentration sind wichtig.
2) Team & Ressourcen: Aktivierung des (eines) Notfallteams und notwendiger Ressourcen!
3) Bestätigung & Analyse: Welche System und Daten sind in welchem Ausmaß betroffen?
4) Eingrenzen & Kappen: Welche Stellen sind betroffen und anschließend zu trennen!
5) Prioritäten setzen: (besser gesetzt haben) und soweit möglich schützen!
6) Kommunikation 1: Jede Kommunikation mit Cyberkriminellen sollten auf ein Minimum beschränkt sein und juristisch begleitet werden!
7) Kommunikation 2: Mitarbeiter müssen über Auswirkungen und Handlungsempfehlungen informiert werden. Kunden müssen ebenfalls zur Schadensminderung informiert werden. Je nach Risiko personenbezogener Daten ist die Aufsicht zu informieren.
8) Forderung(en)?: Zahlung ist nicht immer der besten Weg, zumal nicht sichergestellt ist, dass damit kein weiterer Zugriff besteht. Außerdem bleibt das System infiziert und muss gesäubert werden. Fachlicher Rat ist in jedem Fall einzuholen.
9) Säubern & stärken: Nach dem ersten Angriff sind weitere Angriffe durch Cyberkriminelle wahrscheinlich. Die Sicherheitsvorkehrungen sind so schnell wie möglich zu erhöhen. Dazu gehört auch die Aufklärung aller Beteiligten, fachspezifisch aufbereitet.
10) Vorsorge: Es gilt den Erkenntnisgewinn umzusetzen ob Technik, Penetrationstest oder und vor allem Sensibilisierung der Mitarbeiter zum Schutz und zum frühzeitigen erkennen!

PS: Anregungen zu dem Entwurf für Management, Verantwortlich und Datenschützer nehme ich sehr gerne entgegen und bedanke mich dafür im Voraus.

(4) Zu angrenzenden Themen

(a) Die ganz große Nummer!

FireEye und SolarWinds in den USA sind als Sicherheitsfirmen für Staaten und Großunternehmen bis zu 6 Monate „unterwandert“ worden. Der Angriff konnte nur über bzw. mit Hilfe von Mitarbeiter erfolgen. Für die Interessierten weitergehende Informationen bei LINK: heise-online: Hacker plündern FireEye-Arsenal, LINK: ZEIT-ONLINE: Cyberangriff auf die USA – Der große Rundumschlag (SolarWinds), LINK: ORF.at: Spionageangriff in USA weitet sich aus.

(b) Es geht auch ganz anders

Auszug: *Cyber-Betrug durch Deepfakes ist keine abstrakte Theorie mehr, sondern bereits Realität. Oft reichen schon wenige Daten von einer echten Person um eine täuschend echte Fälschung zu erzeugen. Ein Telefonanruf aus der Konzernzentrale wurde in der britischen Niederlassung zum Geschäftsführer durchgestellt. Es war ein Freitag am späten Nachmittag. „Hello,“ eine selbstbewusste Stimme mit starkem deutschem Akzent ertönte auf Englisch am anderen Ende der Leitung. Der Empfänger hat sein Gegenüber an der Sprechweise erkannt und ließ sofort alles stehen. . … 220.000,00€ teurer Fake - Anruf.*

Allerdings eine Frage: Wie kann man aufgrund eines Anrufs ohne Prüfung auf einem anderen Weg eine ungewöhnliche Zahlung veranlassen. Da fehlt Sensibilität & notwendige Vorsichtsmaßnahmen bzw. Prozess! Link zum Artikel SECURITY INSIDER „KI-Betrug mittels Deepfake“

November 2020 | Zum Datenschutz aufgefallen

Information zum

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann.

*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in),*

Aufsichtsbehörden sind im verpflichtendem Auf – und Ausbau, Verantwortliche wie Privatpersonen und auch Gerichte „*gewöhnen*“ sich langsam an die Pflichten und Rechte aus der EU – DS - GVO. Damit nehmen Neuigkeiten zum Datenschutz nicht ab. Hier finden sich die mir zum Datenschutz aktuell aufgefallenen Nachrichten.

Unter „Inhalt“ sind die Nachrichten übersichtlich aufgeführt. Mit einem Klick gelangen Sie zu einer kurzen Zusammenfassung mit Angabe der Quelle und Link. Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist.

Selbstverständlich können Sie sich auch bei diesen, wie bei allen Fragen zum Datenschutz gerne direkt an mich wenden. Schreiben Sie mir einfach!

Vielen Dank für Interesse

Inhalt

(zusammengestellt von Volker Schroer, zertifizierter Datenschutzbeauftragter)

(1) Serie: Standard-Datenschutzmodell („SDM“).....1

Teil 8: Datenschutzmanagement mit dem SDM.....1

Rechtliche Grundlagen.....1

(a) Vorbereitungen.....1

(b) Spezifizieren und Prüfen.....2

(c) Prozess.....2

(2) Zu Datenschutz.....2

(a) Private Fotos bei Social Media?.....2

(3) Zu Datensicherheit.....2

(a) Datenschutzkonformer Cloud - Service?.....2

(b) Wenn schon Office 365!.....3

(4) Zu angrenzenden Themen.....3

(a) Deepfake: Nackt auf Telegram?.....3

(b) Kontaktlos Karte weg?.....3

(1) Serie: Standard-Datenschutzmodell („SDM“)

Teil 8: Datenschutzmanagement mit dem SDM

(SDM 2.0a S:48 D.4): „Das Datenschutzmanagement ist eine umfassende Methode, um systematisch alle Anforderungen des Datenschutzrechts in einer Organisation umzusetzen. Im Folgenden wird ein Datenschutzmanagement im Zusammenspiel mit dem SDM näher beschrieben.“

Quelle: Link im Bild

Rechtliche Grundlagen

Der Verantwortliche ist für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich und muss den Nachweis erbringen (Führung eines Verarbeitungsverzeichnisses; Dokumentation der technische und organisatorische Maßnahmen; Durchführung der Datenschutz – Folgenabschätzung wo erforderlich und eine kontinuierliche Evaluierung und ggf. Verbesserung). Für die Einhaltung dieser Aufgabenstellung wird der PDCA-Zyklus (Plan, Do, Check, Act) dauerhafter, zyklischer Prozess als Grundlage vorgeschlagen, da auch die Datenschutzprüfungen der Aufsichtsbehörden in der Regel diesem Prozess-Ablauf entsprechen.

(a) Vorbereitungen

1a) Klarheit über die sachlichen Verhältnisse (Wer ist beteiligt und verantwortlich. Welche Daten werden wozu benötigt und wie verarbeitet. Wer kontrolliert und welche Hilfestellungen gibt es).

1b) Zulässigkeit der Verarbeitung (durch Einwilligung, Vertrag, Vorvertragsverhandlungen, rechtliche Verpflichtung, den Schutz lebenswichtiger Interessen, in öffentlichem Interesse, im Interesse des Verantwortlichen und überwiegen dabei die Interessen, Grundrechte und -freiheiten der betroffenen Person.)

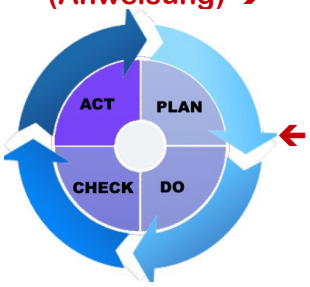
1c) Materiell-rechtliche Beurteilung, d. h. die grundsätzliche Zulässigkeit der Verarbeitungstätigkeit (Anzuwendendes nationales Datenschutzrecht; Legitimität in Bezug auf Zweck und ggf. Übermittlung an Dritte; Erheblichkeit / Notwendigkeit der Datenerhebung;

(SDM 2.0a S:50 D.4.2): „Ausführlichkeit und Detaillierungsgrad insbesondere der Feststellungen zu den sachlichen Verhältnissen werden von Verarbeitung zu Verarbeitung variieren, ebenso wie der Grad der Formalisierung des Vorgehens.“

(b) Spezifizieren und Prüfen

Grundlegende Voraussetzung für die Spezifizierung (und spätere Prüfung) ist die Festlegung, wie die Gewährleistungsziele operationalisiert werden (in Abhängigkeit des Risikos), d. h. nach Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit, Datenminimierung und Belastbarkeit (eben den Gewährleistungszielen). Nach der qualitativen Bestimmung können die technischen und organisatorischen Maßnahme bestimmt werden.

(c) Prozess

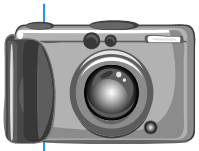
4. Verbessern von erkannten Defiziten bei Grundrechtseingriffen bei der Verarbeitung, den Maßnahmen und / oder des Controlling nach Entscheidung des Verantwortlichen.	(Anweisung) →	1. Planen / Spezifizieren / DSFA Auswahl aller relevanten Daten, IT-Systeme, Prozesse, Schwellenwertanalyse, DSFA usw.
↑ (Erkenntnisse)		↓ (Sollwert)
3. Kontrollieren, prüfen beurteilen Kontrolle des laufenden Betriebs an Hand von Soll / Ist Bilanzen und Beurteilung der Prüfungsergebnisse in Bezug auf rechtliche Vorgaben und Wirksamkeit der Maßnahmen	(Istwert)	2. Implementieren der Verarbeitungsfunktionen, der technischen und organisatorischen Maßnahmen und Herstellung der Prüfbarkeit

Hinweis zur Verwendung abweichender Maßnahmen zum Referenzmaßnahmenkatalog (SDM 2.0a S: 56 - D4.4.3 Abs.3): „Auch wenn diese als grundsätzlich geeignet beurteilt werden können, muss separat geprüft werden, ob sie in ihrer konkreten Ausgestaltung tatsächlich dem festgestellten Risiko entsprechen. *An dieser Stelle hilft das SDM, die Erörterung auf den Nachweis dessen zu fokussieren, dass (oder inwieweit) die getroffene technische oder organisatorische Maßnahme funktional, äquivalent bzw. wirkungsgleich zur Referenzmaßnahme ist.“*

Im Informationsbrief für Dezember folgen die organisatorischen Rahmenbedingungen und der Stand zum Referenzmaßnahmenkatalog

(2) Zu Datenschutz

(a) Private Fotos auf Social Media?



Antwort: „NIE OHNE EINWILLIGUNG!“ Wie der Rechtsanwalt Schäfer unter Anwalt.de ausführt ist die Rechtslage eindeutig und das nicht nur nach dem Datenschutz. Gemäß § 22 KunstUrhG dürfen Bildnisse nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden. Hierzu zählt auch das Posten von Fotos in sozialen Netzwerken oder das Verwenden eines Fotos als Profilbild. Bei Minderjährigen ist die Zustimmung der Erziehungsberechtigten, also beider Elternteile einzuholen (das gilt auch für die Verwandtschaft!).

(3) Zu Datensicherheit

(a) Datenschutzkonformer Cloud - Service?

Nach der Entscheidung des EuGH (Schrems II) zum US – EU – Privacy – Shield sowie den Standard – Vertragsklauseln mit US – Unternehmen nimmt die Diskussion über erlaubtes und unerlaubtes kein Ende. Ob Microsoft Azure & Office, Amazon Web Service oder Google Cloud Plattform, die Analysen nehmen kein Ende und eindeutige Aussagen fehlen bzw. man widerspricht sich. Interessant finde ich da die Aussage von IT – Business: „Warum Sie über die großen Drei hinausschauen sollten“. Die drei Großen bieten zwar hunderte von Services an, aber brauche ich die auch? Rechenzentren und – leistung vieler Alternativen sind identisch. Auch können sie mithalten bei globalen Netzwerken, die in der Lage sind, massive Workloads zu skalieren, regionale Gesetze einhalten und einwandfrei orchestrierte Backups für das „Disaster Recovery“ vorzuhalten. Wenn ich mir über mein Pflichtenheft bewusst bin, kann durch Reduzierung der Komplexität meist noch der Kostenblock gesenkt werden. Für die Interessierten, hier mal beispielhaft 3 Alternativen zum Vergleich von CloudComputing-Insider.

Fazit: Eine Auseinandersetzung mit den „Alternativen“ kann helfen Komplexität zu nehmen und sogar Kosten zu sparen! (Schaden kann es jedenfalls nicht!)

(b) Wenn schon Office 365!

Microsoft betreibt gemeinsam mit der Deutschen Telekom 2 Rechenzentren in Deutschland, und zwar in Frankfurt und Berlin. Die Daten deutscher Neukunden von Office 365 und Dynamics 365 werden bereits seit Februar 2020 in diesen Rechenzentren verarbeitet und gespeichert. Seit kurzem können auch Bestandskunden wechseln, allerdings nur auf Antrag und bis zum 01.05.2021.

Einfach im Admin - Bereich unter Einstellungen der Organisation den Reiter Organisationsprofil aufrufen und dann auf „Data Residency“ klicken. Im dann folgenden Fenster die Checkbox „die ruhenden Kundendaten … bis zum 01.05.2023 nach Deutschland migrieren“ – fertig. So gemäß Microsoft – LINK.

Fazit:

Mit dem Speicherort wird schon mal der Zugriff von US – Behörden auf die dort gespeicherten Daten weitestgehend vermieden. Wie der Pressemitteilung der Aufsichtsbehörden (unter LfDI – Baden-Württemberg) zu entnehmen, ist die (zunächst ablehnende) Prüfung noch nicht abgeschlossen.

(4) Zu angrenzenden Themen

(a) Deepfake: Nackt auf Telegram?

Wie die Datenschutz Nord Gruppe , heise online und auch der Spiegel berichten, haben IT-Sicherheitsexperten der holländischen Sensity B.V. aufgedeckt, dass bis Ende Juli 2020 knapp mehr als 100.000 Frauen Opfer des Missbrauchs Ihrer Fotos wurden. Die Forscher fanden heraus, dass mit einer Deepfake - Software im Messenger - Dienst Telegram („DeepNude“) aus normalen Fotos Nacktbilder generiert, veröffentlicht und in mehreren Telegram - Kanälen verbreitet wurden. Um ein Nacktbild zu generieren, schicken die Täter Fotos ihrer Opfer via Telegram an ein Programm. Nach kurzer Zeit bekommen sie das zu einem Nacktbild manipulierte Foto zurück.

Die italienische Datenschutzaufsichtsbehörde in Rom hat eine Untersuchung gegen Telegram eingeleitet. Für die Behörde in Rom ist eine derartige Bildmanipulation eine gravierende Verletzung der Würde und der Privatsphäre der Menschen. Insbesondere Minderjährige sind von Erpressungen im Rahmen von „revenge porn“ betroffen. Darüber hinaus, sieht die Behörde die Gefahr, dass die Benutzerfreundlichkeit des Programms jeden, der ein Foto im Internet hat, zu einem potentiellen Opfer einer solchen Fälschung macht. Es ist zu erwarten, dass auch die deutschen Aufsichtsbehörden sich einbringen.

(b) Kontaktlos Karte weg?

Der Europäische Gerichtshof hat die Rechte von Verbrauchern gestärkt, wenn sie ihre Bankkarte (oder das Smartphone) mit kontaktloser Bezahlfunktion verlieren. Nach dem neuen Urteil trägt der Kunde nicht das Risiko für Zahlungen, die getätigt werden, nachdem er den Kartenverlust bei der Bank gemeldet hat. So der Spiegel und Anwalt.de

Oktober 2020 | Zum Datenschutz aufgefallen

Information zum

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in),*

Aufsichtsbehörden sind im verpflichtendem Auf – und Ausbau, Verantwortliche wie Privatpersonen und auch Gerichte *„gewöhnen“* sich langsam an die Pflichten und Rechte aus der EU – DS - GVO. Damit nehmen Neuigkeiten zum Datenschutz nicht ab. Hier finden sich die mir zum Datenschutz aktuell aufgefallenen Nachrichten.

Unter „Inhalt“ sind die Nachrichten übersichtlich aufgeführt. Mit einem Klick gelangen Sie zu einer kurzen Zusammenfassung mit Angabe der Quelle und Link. Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist.

Selbstverständlich können Sie sich auch bei diesen, wie bei allen Fragen zum Datenschutz gerne direkt an mich wenden. Schreiben Sie mir einfach!

Vielen Dank für Interesse

Inhalt

(zusammengestellt von Volker Schroer, zertifizierter Datenschutzbeauftragter)

(1) Serie: Standard-Datenschutzmodell („SDM“).....1

Teil 7: Risikobewertung: Zusammenspiel von Schutzbedarf und Schutzniveau.....1

„TOM“, insbesondere bei hohem Datenschutzbedarf.....1

(2) Zu Datenschutz.....2

(a) Schmerzensgeld bei falschem SCHUFA – Eintrag....2

(b) Bußgeld 35,3 Mio. für H&M.2

(3) Zu Datenschutz.....2

(a) Keep it short and simple.....2

(b) BKA – Cybercrime – Lagebild 2019.....3

i) Cybercrime in Deutschland: 3

ii) Ausgewählte Fakten:.....3

iii) Geeignete Schulungsunterlage?!.....3

(4) Zu angrenzenden Themen.....3

(a) Datenschutz – ungutes Gefühl und kein Entgelt!.....3

(1) Serie: Standard-Datenschutzmodell („SDM“)

Teil 7: Risikobewertung: Zusammenspiel von Schutzbedarf und Schutzniveau

Die Eingangsgrafik zu Risikobewertung zeigt, dass ein hoher Schutzbedarf (= Risiko) der Daten durch die Verarbeitung mit entsprechenden technisch – organisatorische Maßnahmen (TOM) im Sinne der DS - GVO gemindert bzw. reduziert werden kann. Das sich aus der Kombination ergebende Schutzniveau muss so hoch sein, dass die verbleibenden Restrisiken durch den Verantwortlichen nachweislich, berechtigt verantwortet werden können; anderenfalls ist eine Verarbeitung mangels Rechtskonformität ausgeschlossen. Was „SO oder SO“ zu dokumentieren ist. Kurz gesagt, wenn bei einer hohen Schadensmöglichkeit (**Datenrisiko = ROT**) aus den Daten mit technisch-organisatorische Maßnahmen eine geringe Eintrittswahrscheinlichkeit (**TOM-Risiko = GRÜN**) erreicht wird, ist die Risikobewertung „überschaubar“ (**Gesamtrisiko = GELB**). Einordnung gemäß Risikobewertungsgrafik.

Als Grundlage für „TOM“ dient der IT – Grundschutz des BSI. Kommt es zu unterschiedlichen Bewertungen mit dem „operativen Datenschutz“ ist entweder die Maßnahme mit dem höheren Schutzbedarf anzuwenden, oder in einer genauere Analyse sind die unterschiedlichen Gründe festzustellen und zu bewerten, wie ein angemessenes Schutzniveau erzielt werden kann. Dabei sind die Anforderungen der DS – GVO maßgeblich.

„TOM“, insbesondere bei hohem Datenschutzbedarf

Zitat SDM 2.0a Seite 46 Punkt D3.4:

Grundsätzlich sind Datenverarbeitungsprozesse und damit die Spezifikation der Datenverarbeitung so zu gestalten, dass, wenn möglich, die Verarbeitung ohne Personenbezug erfolgt oder zumindest die Risiken gemindert werden.

Genanntes Beispiel ist der Einzelabruf von Daten statt Sammelabruf mit nicht benötigten Daten, wenn diese nicht unterdrückt werden können.

Auf dem aktuellen Stand der Technik sind die hier (SDM) ausgeführten und vorgeschlagenen generischen Maßnahmen eine gute Grundlage, um angemessene Maßnahmen für normalen Schutzbedarf zu entwickeln (im SDM 2.0a Punkte D1ff, Seiten 29-35). Bei hohem Schutzbedarf

werden künftig diese Maßnahmen um einen Referenzkatalog* erweitert, der zur Minderung der Risiken empfohlen wird. Zusätzlich sind individuelle Maßnahmen auszuwählen, bestehende Maßnahmen zu verschärfen und die Protokollierung zu erweitern. Zitat (SDM 2.0a Seite 47 D3.4 Nr. 5):

„Transparenz bedeutet, dass eine Verarbeitungstätigkeit anhand von Soll-Ist-Bilanzen prüfbar sein muss. Überprüfbarkeit im Nachhinein bedeutet, dass Protokolldaten erzeugt, gespeichert und verarbeitet werden müssen."

*)Der Referenzkatalog befindet sich noch in der Erarbeitungsphase. Auf der entsprechende Netzseite verweist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) auf eine Sammlung des Landesbeauftragten (LfDI) Mecklenburg-Vorpommerns im Netz. Als verbindliche Versionen (Nr. & Status bei Erstellung der Linkliste) sind hier hinterlegt: Aufbewahren (Nr.11 Okt.2020); Dokumentieren (Nr. 42 Sept.2020); Protokollieren (Nr.43 Sept.2020); Trennen (Nr.50 Okt.2020); Löschen und Vernichten (Nr.60 Sept.2020); Berichtigen (Nr.61 Okt.2020); Einschränken der Verarbeitung (Nr.62 Okt.2020).

Im Informationsbrief für November folgt hier „Datenschutzmanagement mit dem SDM".

(2) Zu Datenschutz

(a) Schmerzensgeld bei falschem SCHUFA – Eintrag

Das Landgericht Darmstadt hat in seinem Urteil vom 19.11.2019 AZ: 13O116/19 eine Bank wegen falscher Schufa-Meldung (= Eintrag) zur einem Schmerzensgeld von 2.000€ wegen Persönlichkeitsrechtsverletzung verurteilt. Nachweisbarer Schaden wäre zusätzlich auszugleichen gewesen. In naher Zukunft wird es wohl mehr Fälle dazu geben, da unter Rechtstipps bei Anwalt.de bereits Hilfe angeboten wird (Link Rechtstipp)

Es gibt dazu schon erste tabellarische Übersichten, wie immaterielle Schäden durch die Gerichte bewertet werden unter: https://dsgvo-schmerzensgeld.de/ . Aktuelle Beispiele daraus sind:

bis 100€ - unerwünschte Werbe – E – Mail: AG Diez, Urt. v. 7.11.2018

bis 10.000€ unzulässige Veröffentlichung von Video / Foto LG Frankfurt, Urt. v. 13.09.2018

bis 8.000€ unzulässige Namensveröffentlichung LG Köln, Beschluss v. 23.12.2019

(b) Bußgeld 35,3 Mio. für H&M

Die Aufsicht in Hamburg (HambBfDI) veröffentlichte am 01.10.2020 ein Bußgeld in Höhe von 35,3 Mio. € wegen Datenschutzverstößen im Servicecenter von H&M (Presse-Link). Seit 2014 kam es bei Teilen der Beschäftigten zu umfangreichen Erfassungen privater Lebensumstände. Nach Abwesenheiten wegen Urlaub und Krankheit kam es zu „Welcome – Back - Talks" bei dem umfangreiche Lebensumstände (Urlaubserlebnisse, Krankheitssymptome, - Diagnosen) ergänzt um „Flurfunk" (von harmlosen Details, über familiäre Probleme bis zu religiösen u. a. Bekenntnissen) teilweise in Aufnahmen und Notizen festgehalten und dauerhaft auf einem Netzlaufwerk gespeichert wurden. Den Zugriff hatten in der Spitze bis zu 50 Führungskräfte. Auffällig wurde es durch einen „Konfigurationsfehler", durch den einige Stunden ein unternehmensweiter Zugriff bestand.

(3) Zu Datensicherheit

(a) Keep it short and simple

…, denn komplex wird es dahinter von ganz alleine. In dem Artikel „Keep it simple – zurück zu den Grundlagen der Cybersicherheit" sieht der Autor Thomas LaRock (Autor, Sprecher, Datenexperte) die wichtigen Verteidigungslinien weniger bei den „vermeintlichen" Wundermitteln von künstlicher Intelligenz bis Blockchain, sondern macht die Grundlagen an 3 Punkten fest.

1. Kennwort schützt, wenn … es in Verbindung mit einer zweistufigen Authentifizierung und einem Passwort – Manager (Vermeidung einfacher Passwörter) genutzt wird.
2. Geschulte Mitarbeiter, wenn … grundlegende Sicherheitspraktiken für E – Mail, Datenschutz und Privatsphäre fester Bestandteil bei Neueinstellungen sind, ohne zu sehr in die Tiefe zu gehen.

Regelmäßige Information der Mitarbeiter über neue Bedrohungen und Trends um das Bewusstsein langfristig aufrecht zu halten ohne zu „langweilen“ mit immer der gleichen Schulung. Ergänzt durch die IT mit Netzwerküberwachungen bis hin zu umfassenden Back – End – Abwehrmaßnahmen. Der Mitarbeiter ist zwar die erste, sollte aber nicht die einzige Abwehrlinie sein!

3. Wir sind sicher, wenn … wir ständig vermuten kompromittiert zu sein oder zu werden und immer für den Notfall gewappnet sind (Prozesse, Backup – Regeln, Testläufe, Stand der Technik).

(b) BKA – Cybercrime – Lagebild 2019

Wer hier „trockenen Lesestoff“ vermutet, der wird enttäuscht sein. In sehr angenehmer, kurzweiliger und verständlicher Form werden die wesentlichen Betrugsmaschen kurz erklärt (Was, Wie, aktuelle Beispiele). Ob ID-Theft mittels SIM-Swapping, Erpressung mittels GrandCrab, Manipulationen mittels AZORult oder njRat, Mobil – Malware – Varianten oder Jackpotting alles kurz und an Hand von Grafiken und konkreten Beispielen kurz erklärt. Prägende Angriffe in jedem Monat 2019 werden kurz und übersichtlich dargestellt.

Schaubild Report Seite 6

Markant und interessant für den geneigten Leser ist auch die Darstellung zur Industrialisierung der Untergrundökonomie, ***CCaaS = Cybercrime-as-a-Service*** mit Marktplätzen, Shops, Foren, Bewertungsportalen und Newsblocks. Von den Fachbegriffen sollten man sich nicht schrecken lassen, die werden verständlich erklärt.

i) Cybercrime in Deutschland:

Die Professionalität von Cyberkriminellen steigt und basiert auf kriminellen, global vernetzten, international agierenden, höchst organisierten, arbeitsteiligen Wertschöpfungsketten. Ransomware bleibt die größte Bedrohung für Unternehmen und die Anzahl wie Intensität von DDoS – Angriffen steigt rapide an. Die wichtigsten Schutzmechanismen gegen Cybercrime sind weiterhin sensible Internetnutzer.

ii) Ausgewählte Fakten:

Spam – Mails haben sich gegenüber 2018 fast verdreifacht bei über 1 Milliarde Malware – Familien, davon neue Varianten in 2019 ca. 114 Mio., was ca. 312.000 pro Tag entspricht. Drei von vier Unternehmen wurden 2019 Opfer von Angriffen gegenüber zwei von vier Unternehmen noch in 2017. Der Schaden beläuft sich in 2019 auf ca. 103 Mrd. €.

iii) Geeignete Schulungsunterlage?!

Zur regelmäßigen Sensibilisierung eignen sich Auszüge für eine Präsenzveranstaltung (aktuelle, prägende Angriffe, Betrugsarten mit Erklärung und aktuellen Beispielen, Organisation der Täterökonomie und wichtiges kompakt zum Schutz) sowie zum Nachlesen für die Interessierten. Statt mit Standard – Wiederholung kann mit aktuellem Bezug Aufmerksamkeit erzeugt werden.

LINK: Bundeslagebild Cybercrime 2019 BKA

(4) Zu angrenzenden Themen

(a) Datenschutz – ungutes Gefühl und kein Entgelt!

Letzten Monat hatte ich über eine Studie berichtet, in der die Verbraucher für ein guten Datenschutz auch etwas oder mehr bezahlen würden. IT-Business berichtet am 12.10.2020 von einer Eos – Umfrage, nach der jeder dritte Verbraucher in Deutschland bereit sei, seine Daten zu verkaufen (bereits unter 50€). Einzig festzuhalten ist, so wie jetzt sollte es nach den Verbrauchern dann wohl nicht bleiben (ungutes Gefühl und kein Geld).

September 2020 | Zum Datenschutz aufgefallen

Liebe(r) Leser(in),*

Aufsichtsbehörden sind im verpflichtendem Auf – und Ausbau, Verantwortliche wie Privatpersonen und auch Gerichte „*gewöhnen*“ sich langsam an die Pflichten und Rechte aus der EU – DS - GVO. Damit nehmen Neuigkeiten zum Datenschutz nicht ab. Hier finden sich die mir zum Datenschutz aktuell aufgefallenen Nachrichten.

Unter „Inhalt“ sind die Nachrichten übersichtlich aufgeführt. Mit einem Klick gelangen Sie zu einer kurzen Zusammenfassung mit Angabe von Quellen und Link. Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist.

Selbstverständlich können Sie sich auch bei diesen, wie bei allen Fragen zum Datenschutz gerne direkt an mich wenden. Schreiben Sie mir einfach!

Vielen Dank für Interesse

Information zum

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

Inhalt

(zusammengestellt von Volker Schroer, zertifizierter Datenschutzbeauftragter)

(1) Serie: Standard-Datenschutzmodell („SDM“).....1

Teil 6: Risiken & Schutzbedarf..1

(a) Risiken für Betroffene.....1

(b) Risikobetrachtung.....2

i) Schwellwert – Analyse.....2

ii) Risikoidentifikation.....2

iii) Risikobewertung.....2

(2) Zu Datenschutz.....2

(a) Schrems II hat was von Shrek(2).....2

(b) MS 365 & Schrems II (?).....3

(3) Zu Datensicherheit.....3

(a) Die IT im Schatten - finden & integrieren.....3

(b) Angriff aus der Espresso – Maschine.....3

(4) Zu angrenzenden Themen.....3

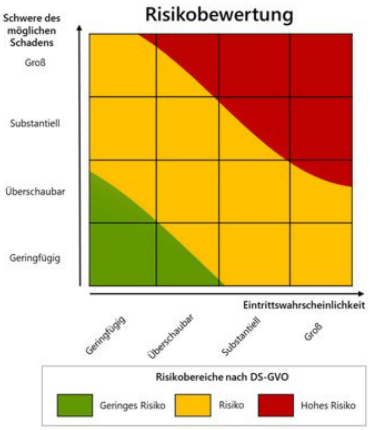
(a) Bezahlen für Datenschutz & -sicherheit?.....3

(1) Serie: Standard-Datenschutzmodell („SDM“)

Teil 6: Risiken & Schutzbedarf

Quelle: Link im Bild

Risiko im Sinne der DS-GVO ist die Möglichkeit eines Schadeneintritts für die Rechte und Freiheiten einer oder mehrerer natürlicher Personen, einschließlich der ungerechtfertigten Beeinträchtigung oder zu einem solchen Schaden führen kann. Ausführliche Beschreibung von möglichen Schäden im Erwägungsgrund (75) der DS-GVO (physisch, materiell, immateriell, Diskriminierung, Identitätsdiebstahl & -betrug, Rufschädigung, finanzieller Verlust um nur einige zu nennen). Die Risikoermittlung erfolgt über zwei Dimensionen, (1.) der Schwere des Schadens(Y-Achse) und (2.) der Eintrittswahrscheinlichkeit (X-Achse). Grundsätzlich unterscheidet Verordnung / Gesetz und Aufsicht nur in die Kategorien geringes bis normales Risiko (grün, gelb) und hohes Risiko (rot). Bei „ROT“ ist eine Datenschutz – Folgenabschätzung (DS - FA) zwingend. Bleibt auch nach DS - FA die Stufe „ROT“ ist VOR Verarbeitung die Aufsicht zu einzuschalten (DS-GVO Art.35, 36).



(a) Risiken für Betroffene

Im Gegensatz zum allgemeinen und IT – Risikomanagement besteht im Datenschutz grundsätzlich die Pflicht, entstehende Risiken mit geeigneten und angemessenen technisch – organisatorischen Maßnahmen auf eine angemessenes Schutzniveau zu reduzieren (X-Achse)! Es ist NICHT ZULÄSSIG auf Behandlung und Anforderung der Grundsätze nach Art. 5 DS-GVO zu verzichten und Risiken daraus in Kauf zu nehmen. RISIKO - AKZEPTANZ oder RISIKO - TRANSFER (z. B. bekannt aus der Informationssicherheit) stehen den Verantwortlichen im Datenschutz NICHT ZUR VERFÜGUNG. Erst wenn im Interesse des Betroffenen ein angemessenes Schutzniveau (grün, gelb) erreicht wird, können verbleibende Risiken durch den Verantwortlichen akzeptiert werden.

(b) Risikobetrachtung

i) Schwellwert – Analyse

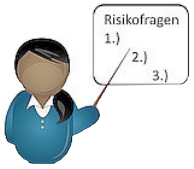
Die Schwellwert – Analyse dient der Identifikation eines voraussichtlich hohen Risikos der Verarbeitungstätigkeit und beinhalte folgende (Prüf-) Schritte:

- ✗ Alle Verarbeitung nach Art. 35 Abs.3 lit.a-c DS-GVO wie (a) systematische, umfassende, automatisierte Bewertung persönlicher Aspekte (Profiling), (b) umfangreiche Verarbeitung besondere Kategorien von oder strafrechtliche Daten (Art. 9 Abs.1 und Art. 10 DS-GVO) und (c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.
- ✗ Auf der „Muss-Liste“ (auch Positiv- bzw. Negativliste) gem. Art.35 Abs. 4 DS-GVO. Für den nicht-öffentlichen Bereich wird diese Liste von der Datenschutzkonferenz veröffentlicht unter diesem LINK. Darin enthalten u. a. biometrische Daten wie Fingerabdruckscanner, medizinische Daten wie DNA-Tests, Finanz- und Bonitätsdaten wie Zahlungsverhalten, Insolvenzliste, Sensordaten wie GPS, Bluetooth, NFC, Funk, Scoring, Profiling u. s. w.
- ✗ Nach den Leitlinien der Datenschutzgruppe nach Artikel 29 (WP248 Rev.01) reichen zwei zutreffende Kriterien (bzw. auch schon eins) aus. Die Kriterien sind:

() Scoring / Evaluation	() Rechtswirksame, automatische Entscheidungsfindung
() Systematische Überwachung	
() Datenverarbeitung in großem Umfang	() Vertrauliche, höchst persönliche Daten
() Abgleich / Zusammenführen von Daten	() Daten von schutzbedürftigen Personen
() Innovative / neue Technologien (KI)	() Hinderung an Rechts- u/o Vertragsausübung

- ✗ Allgemein nach Erwägungsgrund (76) DS-GVO, objektive Risikobestimmung nach Art, Umfang und Zweck der Verarbeitung

ii) Risikoidentifikation



Drei + 1 Fragen:

I. Welche Schäden können für betroffene Personen bei der Datenverarbeitung auftreten?

II. Wodurch kann es zu einem Schaden kommen?

III. Welche Handlungen und Umstände können das Schadenereignis auslösen?

- ◆ Welche technisch – organisatorischen Maßnahmen sind zum Schutz der Daten getroffen und sind die angemessen und ausreichend? (z. B. an Hand IT – Grundschutz)

iii) Risikobewertung

(Zitat: DSM 2.0a S:44:) „Es ist die Aufgabe des Verantwortlichen und ggfs. des Auftragsverarbeiters, die identifizierten Risiken für die betroffenen Personen zu analysieren und einzustufen ... die Eintrittswahrscheinlichkeit der identifizierten Risiken nach objektiven Maßstäben bestimmen und dokumentieren.“

Im Informationsbrief für Oktober folgen hier die Zusammenfassung der Punkte: „Risikobewertung im Zusammenspiel von Schutzbedarf und Schutzniveau“ sowie „TOM – insbesondere bei hohem Risiko“.

(2) Zu Datenschutz

(a) Schrems II hat was von Shrek(2)

Schrems II hat etwas von „tollkühner Held“ ist aber kein Film (von DreamWorks), sondern ein derzeit viel diskutiertes Urteil des EuGH über Datenverarbeitung in Ländern außerhalb der EU, insbesondere in den USA. Näheres bereits im Informationsbrief Juli 2020 unter 2.a) hier verlinkt. Es betrifft ja nicht nur die großen US – Service- / Produktanbieter wie Google, Facebook, Microsoft, Amazon, sondern viele Geschäftsbeziehungen und das nicht nur in den USA (z.B. auch Großbritannien, Inden u.a.). Die großen Fragen sind: „Was geht jetzt (?) und wie geht das (?)“. Da die Aufsichtsbehörden dazu aktuell kein so ganz einheitliches Verständnis kommunizieren und bereits über 100 Beschwerden erfolgten, hat das EDPB (Europan Data Protection Board = EDSA Europäischer Datenschutzausschuss) eine Task - Force zur eindeutigen Klärung eingesetzt (LINK: Pressemitteilung BfDI).

Für das zwischenzeitliche „WIE“ stellt die Aufsicht in Baden-Württemberg in einer Pressemitteilung vom 24.08.2020 eine Orientierungshilfe zur Verfügung (jeweils verlinkt). Kurz gesagt, sollte wie in der Juli – INFO ausgeführt kein gültiger EU – Angemessenheitsbeschluss, oder geeignete Garantien mit Standardvertragsklausel oder eine restriktive zu handhabende Einwilligung nach Art. 49 DS – GVO vorliegen, wird die Aufsicht prüfen, ob wirklich keine Alternativen wie Anonymisierung, geeignete Verschlüsselung vor Transfer u. ä. glaubhaft zur Verfügung stehen und dies „wohlwollend“ berücksichtigen. Die Orientierungshilfe beinhaltet auch eine gute Checkliste was zu tun ist (z.B. Anpassung der Datenschutzerklärung, Information Betroffener usw.)

(b) MS 365 & Schrems II (?)

Microsoft (vorml. Office) 365 ist bereits seit letztem Jahr in der Kritik der Aufsichtsbehörden. Ende 2018 veröffentlichte die Niederländische Aufsichtsbehörde eine Analyse zu Office / Microsoft 365 mit dem Ergebnis: „Nicht datenschutzkonform zu betreiben“. Kern der Kritik, es waren 8 Schwerpunkte sind das Sammeln von Telemetrie- und Diagnose- mit Nutzerdaten und die Möglichkeit der Einbindung von Social – Media – Plattformen, was soweit möglich abzuschalten ist. Bearbeitung von sensibel Daten nur mit Verschlüsselung (z. B. Lockbox). Online und Mobil wird als sehr kritisch angesehen. Der Einschätzung ist auch die deutsche Aufsicht im wesentlich gefolgt.

Nach dem Urteil „Schrems II“ sind viele Aufsichtsbehörden zu einem Verbot mangels datenschutzkonformen Betriebs übergegangen. Wie „heise-online“ berichtet, sollen die Experten eines Unterarbeitskreises der Datenschutzkonferenz (DSK) im Rahmen ihrer monatelangen Untersuchung zu dem Schluss gekommen sein, dass "kein datenschutzgerechter Einsatz von Microsoft 365 möglich sei". Der Bericht ist noch nicht veröffentlicht, da sich bisher nicht alle Landesbehörden einig sind.

Update: *Lt. Heise Online soll Microsoft in einem Blogbeitrag zu Exchange nebenbei erwähnt haben, dass im Herbst 2021 eine Office Version für Windows (lokal also) auf den Markt kommen soll. Anmerkung: „Zufall oder Vorsorge?“*

(3) Zu Datensicherheit

(a) Die IT im Schatten - finden & integrieren

Es sind ja nicht nur die Social – Media – Plattformen, deren Einbindung in die IT des Unternehmens kritisch zu prüfen bzw. zu verbieten sind. Nicht selten kommt es vor, dass Abteilungen oder Nutzern direkt (und an der IT vorbei) Services angeboten (z. B. Cloud – Speicher und Cloud – Programme) und eben auch genutzt werden (= Schatten – IT). Deshalb ist zumindest eine Genehmigungsregelung festzulegen, zu kommunizieren und in regelmäßigen Abständen einen Bestandsaufnahme abzufragen. Natürlich sind auch technische Tools zum „aufspüren“ der Schatten – IT erhältlich.

(b) Angriff aus der Espresso – Maschine

Nach dem Jahresbericht „The state of IoT Cybersecurity in 2020 by Forescout Research Labs“ sind die größten Einfallstore bei IoT im Unternehmen die Zugangskontrollen (Platz 1.), Heizung / Lüftung / Klimatechnik (Platz 2), gefolgt von Kameras / Drucker (Platz 3).

Welche Gewohnheiten haben Arbeitnehmer im Home - Office? Dieser Frage ging Trend Micro in der Studie nach, für die über 13.000 Remote - Mitarbeiter in 27 Ländern weltweit befragt wurden. Danach greifen 40 – 45% der Mitarbeiter im Home – Office mit eigen Geräten auf Unternehmensdaten und -anwendungen zu. Mit allen Risiken die damit verbunden sind, da nicht sichergestellt ist, dass ein entsprechendes Schutzniveau garantiert ist (für Geräte, Netzwerk und eingebundene IoT). Ein Beispiel gefällig: Wenn das Aquarium das Casino hackt;

(4) Zu angrenzenden Themen

(a) Bezahlen für Datenschutz & -sicherheit?

Aus einer SINUS – Umfrage aus 2018 wissen wir, das 92% der Deutschen die Sicherheit ihre Daten eher (38%) bzw. sehr wichtig (54%) ist. IT – Business berichtet von einer aktuellen OpenText – Umfrage: „Verbraucher würden mehr bezahlen für mehr Datenschutz“. Aber wie „bezahlbares Vertrauen“ aufbauen? Als „Datenschützer“ mag ich voreingenommen sein, aber „in rechtmäßiger Weise … nach Treu und Glauben … Transparent … in einer klaren und einfachen Sprache“ hört sich nach DS – GVO an, ist es auch!

August 2020 | Zum Datenschutz aufgefallen

Information zum

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in),*

Aufsichtsbehörden sind im verpflichtendem Auf – und Ausbau, Verantwortliche wie Privatpersonen und auch Gerichte „*gewöhnen*“ sich langsam an die Pflichten und Rechte aus der EU – DS - GVO. Damit nehmen Neuigkeiten zum Datenschutz nicht ab. Hier finden sich die mir zum Datenschutz aktuell aufgefallenen Nachrichten.

Unter „Inhalt“ sind die Nachrichten übersichtlich aufgeführt. Mit einem Klick gelangen Sie zu einer kurzen Zusammenfassung mit Angabe von Quellen und Link. Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist.

Selbstverständlich können Sie sich auch bei diesen, wie bei allen Fragen zum Datenschutz gerne direkt an mich wenden. Schreiben Sie mir einfach!

Vielen Dank für Interesse

Inhalt

(zusammengestellt von Volker Schroer, zertifizierter Datenschutzbeauftragter)

(1) Serie: Standard-Datenschutzmodell („SDM“).....1

Teil 5: Nachtrag zur Umsetzung der Gewährleistungsziele.....1

(h) Gewährleistungsziele als Design - Strategie.....1

(i) Verarbeitungstätigkeiten.....1

i) Ebenen.....2

ii) Zweck.....2

iii) Komponenten.....2

(2) Zu Datenschutz.....2

(a) Bargeldlos bezahlen vs. Datenschutz.....2

(b) Mitarbeiter/innen - beschützte Wesen.....2

i) Mitarbeiterdaten sind.....2

ii) Eine Checkliste.....3

iii) Datenschutz bei Internetrecherche.....3

iv) Aufbewahrungsfristen bzw. Löschpflichten.....3

(3) Zur Datensicherheit.....3

(4) Zu angrenzenden Themen.....3

(a) Die Steuer - ID & Corona?..3

(1) Serie: Standard-Datenschutzmodell („SDM“)

Teil 5: Nachtrag zur Umsetzung der Gewährleistungsziele

Der Hinweis war: **„Wegen der allgemeinen Gültigkeit ist sicherlich eine sinnvolle Ausprägung** der Maßnahmen **je nach** Verarbeitung, Größe, Umfang und Art der Daten **zu berücksichtigen“**. Zitate:

„In der datenschutzrechtlichen Beurteilung müssen Juristen und Informatiker deshalb eine gemeinsame Sprache finden, um sicherzugehen, dass diese rechtlichen Anforderungen auch tatsächlich technisch und organisatorisch umgesetzt werden. Generische Maßnahmen werden sie durch die Gewährleistungsziele unterstützten. Anführung von typischen, technischen und organisatorischen Referenzmaßnahmen „die in der Datenschutzpraxis vieler Datenschutzaufsichtsbehörden seit vielen Jahren erprobt sind“. [… angemessen und praktikabel fände ich noch gut]

In Teil 4 behandelte:

(a) Datenminimierung	*(b) Verfügbarkeit*	*(c) Integrität*
(d) Vertraulichkeit	*(e) Nichtverkettung*	*(f) Transparenz*
(g) Intervenierbarkeit	*(h) Design – Strategie*	*(i) Verarbeitungstätigkeiten*

(h) Gewährleistungsziele als Design - Strategie

In der Planung und Entwicklung, vor der Freischaltung einer Anwendung, sollten die Grundsätze der datenschutzfreundliche Voreinstellung (Data Protection by Default) und der datenschutzfreundlichen Technikgestaltung (Data Protection by Design) Einzug nehmen.

(i) Verarbeitungstätigkeiten

Art.30 DS-GVO verwendet „Verarbeitungstätigkeiten“ als zentralen Begriff für das Datenschutzmanagement und listet die vom Verantwortlichen im „**Verzeichnis der Verarbeitungstätigkeiten**“ zu führenden Angaben auf (gem. dem zentralen Begriff „Verarbeitung“ in Art.4 Abs.2 DS-GVO):

- ✔ Name und Kontaktdaten Verantwortlicher, Vertreter, Datenschutzbeauftragter.
- ✔ Zwecke der Verarbeitungen und Beschreibung der Kategorien, Betroffenen, Empfänger, Übermittlungen, Drittländer und internationale Organisationen.
- ✔ Vorgesehene Fristen zur Löschung
- ✔ Allgemeine Beschreibung der technisch – organisatorischen Maßnahmen (Art.32 Abs.1 DS-GVO) kurz „TOM“

Allerdings stellen diese Mindestanforderungen noch keine ausreichende Dokumentation im Sinne der Transparenz nach Art.5 Abs.2 DS-GVO dar. Es stellt sich die Frage, ob die richtigen Maßnahmen zweckgemäß ausgewählt und mit der korrekten „Wirkintensität“ betreiben werden.

i) Ebenen

Nach den Erfahrungen der Aufsichtsbehörden hat sich die Darstellung zumindest in 3 Ebenen bewährt:

Ebene 1: Darstellung der datenschutzrechtlichen Konformität (Prozessnotwendige Daten)

Ebene 2: Praktische Umsetzung (Sachbearbeitung, Applikation, Verfahren)

Ebene 3: IT – Infrastruktur einschl. Sicherungskonzept (TOM)

ii) Zweck

Zur Darstellung des rechtskonformen Zwecks sollte eine Zweckabgrenzung bzw. Zwecktrennung vorgenommen werden um strittige Deutungen zu vermeiden. Der Aspekt der Zweckbindung sollte die geeignete Funktionalität im direkten Verarbeitungsprozess (horizontale Zugriffe) und im Umfeld (vertikale Zugriffe, z. b. IT – Services) darlegen.

iii) Komponenten

Bei der Modellierung von Verarbeitungstätigkeiten ergeben sich aus der DS-GVO folgende drei Komponenten:

1. Personenbezogenen Daten (Festlegung des Schutzbedarfs der Person)
2. Technische System und Dienste (Ergänzende Daten aus Systemen, z. B. Datums- und Ortsangaben bei Onlineerfassung, Bild & Tonaufnahmen u. ä.)
3. Technische, organisatorische und personelle Prozesse (Schnittstellen, Drittübermittlung, Auftragsverarbeitung)

✍ Besondere Beachtung bei den drei Komponenten finden die Datenformate, die Schnittstellen und die durchgehenden Verantwortlichkeiten.

Hier folgt in den nächsten Informationsbriefen nach und nach eine kurze Zusammenfassungen der einzelnen Inhalte. Im nächsten Informationsbrief „Teil 6“ Risiken und Schutzbedarf.

(2) Zu Datenschutz

(a) Bargeldlos bezahlen vs. Datenschutz

Während Zahlungsdienstleister wie Banken und Kreditkartenorganisation die Daten lediglich zur Zahlungsabwicklung nutzen, dürften die Daten bei Facebook und Google eher eine Analyse mittels Algorithmus unterliegen. Interessante Kurznotiz von www.datenschutz-notizen.de

(b) Mitarbeiter/innen - beschützte Wesen

Die DSGVO legt fest, dass personenbezogene Daten – also auch Mitarbeiterdaten – nur dann verarbeitet werden dürfen, wenn dies durch eine bestimmte Rechtsgrundlage oder eine Einwilligung des Mitarbeiters erlaubt ist. Diese Rechtsgrundlage findet sich im § 26 Bundesdatenschutzgesetz (BDSG) sowie im Erwägungsgrund 155 und Art.88 DS-GVO . Das BDSG bestimmt, dass Arbeitgeber auch ohne Einwilligung der Mitarbeiter solche personenbezogenen Daten verarbeiten dürfen, die für die Aufnahme, Durchführung oder Beendigung eines Arbeitsverhältnisses erforderlich sind.

i) Mitarbeiterdaten sind

beispielhaft Vor- und Nachname, Wohnort, Kontaktdaten, Geburtsdatum, Religion, Finanzamt, Krankenkasse, Staatsangehörigkeit, Personalnummer, Gehalt, Bankverbindung, beruflicher Werdegang, evtl. Abmahnungen u. ä., aber nur wenn diese zur Durchführung des Beschäftigungs-

verhältnisses erforderlich sind. Für alle nicht notwendigen Mitarbeiterdaten Bedarf es einer freiwilligen Einwilligung (mit !!!).

ii) Eine Checkliste

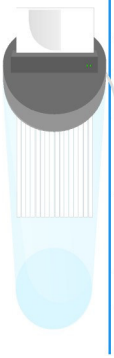
- Informationspflicht (Art.13, 14 DS-GVO): Pflicht zur Information über Art, Zweck, Speicherdauer und Empfänger der erhobenen Daten, Datenschutzbeauftragter und die Rechte als Betroffener (schriftlich, Intranet bei Zugriffsberechtigung, E-Mail Bestätigung bei Bewerbungen, „Opt-In“ bei Portal).
- Verpflichtung zum Datenschutz (Art.29, 5 DS-GVO): Gleichlaufend muss sich der Mitarbeiter auf die Einhaltung der Datenschutzregeln verpflichten.
- Betriebsvereinbarung (Art.88 DS-GVO und §26 Abs.4 BDSD): Eine „Kollektivvereinbarung“ kann auch Grundlage für die Verarbeitung sein, wenn diese Datenschutzkonform (DS-GVO) ist.
- Einwilligung (Art.7 DS-GVO; §26 BDSG): Aufklärung / Informationspflicht konkret, in klarer und einfacher Sprache über alle Daten, mindestens der für das Beschäftigungsverhältnis nicht notwendigen Daten. Die Einwilligung hat freiwillig, unabhängig vom Beschäftigungsverhältnis zu erfolgen. Dazu lautet es im Gesetze: „*Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen*“.
  - *Mitarbeiterfotos:* Eine pauschale Einwilligung für die Verwendung von Fotos ist unwirksam. Denn die Datenverarbeitung muss laut DSGVO immer zweckgebunden erfolgen. Das bedeutet, dass der Betroffene immer vor der Veröffentlichung eines Fotos einer Plattform gefragt werden muss. Die Zustimmung muss aber nicht mehr handschriftlich erfolgen. Es reicht, wenn die Einwilligung per E-Mail erteilt wird. Eine Unterschrift ist damit nicht mehr nötig. Und die Einwilligung kann jederzeit Widerrufen werden. *Quelle: Anwalt.de*

iii) Datenschutz bei Internetrecherche

… darf nicht vergessen werden – ein umstrittenes Thema. Allgemein zugängliche Daten dürfen erhoben werden, wenn keine Persönlichkeitsrechte entgegenstehen. Das liegt in den Begriffen „erforderlich“ und „angemessen“. Persönliche Bereiche, z. B. in Sozialen Netzwerken sind tabu. Die Bundesaufsicht hat bereits eine Facebook Recherche angemahnt. In mancher AGB eines Sozialen Netzwerkes ist eine Verbot für Personalerhebungen verankert. Die Persönlichkeitsrecht sind immer zu beachten. Höchstpersönliche Daten (z. B. finanzielle Situation, Religion, Rasse u. s. w.) dürfen grundsätzlich nicht erfasst werden.

iv) Aufbewahrungsfristen bzw. Löschpflichten

Datenerhebung, Verarbeitung und Speicherung unterliegen strengen inhaltlichen und zeitlichen Begrenzungen (siehe DSGVO Art.5 Zweckbindung und Art.17 Recht auf Löschung) mit Ausnahme einer rechtlichen Verpflichtung (Art.17 Abs.3 lit.b DS-GVO). Die wesentlichen Fristen sind:



6 Monate: Bewerberunterlagen (2 Monate Ausschlussfrist §15 AGG; plus 3 Monate Klagefrist §61b Abs.1 ArbGG und Sicherheitszuschlag 1 Monat)
2 Jahre: Als Nachweis über die Einhaltung von Schutzvorschriften, z. B. §16 Abs.2 ArbZG – Arbeitszeiten.
3 Jahre: Anspruch auf Arbeitszeugnis für eingestellte Bewerber / Mitarbeiter nach §109 GewO und §§195,199 BGB Verjährungsfristen.
6 Jahre: Aufbewahrungspflicht aus Steuer- und Sozialrecht nach §147 AO.
10 Jahre: Aufbewahrungspflicht aus Steuer- und Handelsrecht nach §147 AO.
Hinweis: Diese Daten dürfen für keinen anderen Zweck weiter verwendet werden.

Weitere Quellen:
Hauf Bewerberdatenschutz;
Art.17 DS-GVO;
Blog Kliemt.AR;

(3) Zur Datensicherheit

(4) Zu angrenzenden Themen

(a) Die Steuer - ID & Corona?

Hat doch die Bundesregierung mit dem Corona – Hilfspaket auch eine Ausweitung der Steuer – ID zur Bürger – ID für das e-Goverment beschlossen – Datenschutzalarm!
Quelle: c't Magazin & Artikel des Bundesbeauftragten BfDI

Juli 2020 | Zum Datenschutz aufgefallen

Information zum
Datenschutz - Service
oder Fragen per Mail an:
Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in),*

Aufsichtsbehörden sind im verpflichtendem Auf – und Ausbau, Verantwortliche wie Privatpersonen und auch Gerichte *„gewöhnen“* sich langsam an die Pflichten und Rechte aus der EU – DS - GVO. Damit nehmen Neuigkeiten zum Datenschutz nicht ab. Hier finden sich die mir zum Datenschutz aktuell aufgefallenen Nachrichten.

Unter „Inhalt“ sind die Nachrichten übersichtlich aufgeführt. Mit einem Klick gelangen Sie zu einer kurzen Zusammenfassung mit Angabe von Quellen und Link. Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist.

Selbstverständlich können Sie sich auch bei diesen, wie bei allen Fragen zum Datenschutz gerne direkt an mich wenden.

Vielen Dank für Interesse

Inhalt

(zusammengestellt von Volker Schroer, zertifizierter Datenschutzbeauftragter)

(1) Serie: Standard-Datenschutzmodell („SDM“).....1
Teil 4: Systematisierung und praktische Umsetzung der Gewährleistungsziele.....1
(a) Datenminimierung.....1
(b) Verfügbarkeit.....1
(c) Integrität.....2
(d) Vertraulichkeit.....2
(e) Nichtverkettung.....2
(f) Transparenz.....3
(g) Intervenierbarkeit.....3
(2) Zu Datenschutz.....3
(a) EuGH Entscheidung (Juni) „kippt Datendeal mit USA“ ? !...3
(b) Italien weist den Weg.....4
(c) Und es trifft nicht nur die „Großen“!.....
(3) Zu Datensicherheit.....4
(a) PS: Zur EuGH Entscheidung für die Cloud:.....4
(b) Zeitlos wichtig: „Das Pizza-Passwort“.....4
(4) Zu angrenzenden Themen.....4
(a) Echt jetzt?: "Bundesamt für Krisenschutz und Wirtschaftshilfe".....4

(1) Serie: Standard-Datenschutzmodell („SDM“)

Teil 4: Systematisierung und praktische Umsetzung der Gewährleistungsziele

Entgegen der Agenda im SDM habe ich die Systematisierung (rechtlicher Ansatz) und die generischen Maßnahmen (praktische Umsetzung) unter den 7 Gewährleistungszielen zusammengeführt. **Wegen der allgemeinen Gültigkeit ist sicherlich eine sinnvolle Ausprägung** der Maßnahmen **je nach** Verarbeitung, Größe, Umfang und Art der Daten **zu berücksichtigen**. Zitate:

„In der datenschutzrechtlichen Beurteilung müssen Juristen und Informatiker deshalb eine gemeinsame Sprache finden, um sicherzugehen, dass diese rechtlichen Anforderungen auch tatsächlich technisch und organisatorisch umgesetzt werden. Generische Maßnahmen werden sie durch die Gewährleistungsziele unterstützten. Anführung von typischen, technischen und organisatorischen Referenzmaßnahmen „die in der Datenschutzpraxis vieler Datenschutzaufsichtsbehörden seit vielen Jahren erprobt sind“. [… angemessen und praktikabel fände ich noch gut]

(a) Datenminimierung

>Systematisierung: Das Minimierungsgebot erstreckt sich nicht nur auf die Menge der verarbeiteten Daten, sondern auch auf den Umfang der Verarbeitungen, die Speicherfristen und die Zugänglichkeit (je weniger und desto kürzer, um so besser).

Die rechtlichen Anforderungen ergeben sich aus DS - GVO Art.5 Abs.1 lit.c (Minimierung); Art.5 Abs.1 lit.e (Begrenzung); Art.25 Abs.2 (datenschutzfreundliche Voreinstellung)

>Praktisch: Reduzierung um alle nicht mehr notwendigen Daten,

wie einzelne Attribute, Verarbeitungsoptionen, Datenisolierung, Pseudonymisierung, Anonymisierung, nicht notwendige Datenmasken, Löschkonzept u.ä.

(b) Verfügbarkeit

>Systematisierung: Unverzüglicher Zugriff auf und Auffindbarkeit der (personenbezogenen) Daten und der Verarbeitung im ordnungsgemäß vorgesehenen Prozess, einschließlich einer angemessenen, gut verständlichen Darstellung für die Person (Datenmanagement – Systeme, Datenbanken, Suchfunktionen). Ein Schutz und zügiger Zugriff auch bei physischen oder

technischen Zwischenfällen und bei hoher Systemlast. Bei Ausnahme eines Störfalles sind und werden Maßnahmen zur Behebung getroffen.

Die rechtlichen Anforderungen ergeben sich aus der DS – GVO Art.32 Abs.1 lit.b (Verfügbarkeit, Belastbarkeit); Art.32 Abs.1 lit.b, c (Wiederherstellbarkeit); Art.33 Abs.3 lit.d & Art.34 Abs.2 (Behebung, Abmilderung von Störungen/Verletzungen)

>Praktisch:

Sicherungskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien gemäß eines getesteten Konzeptes.

(c) Integrität

>Systematisierung: Sicherstellung der technischen Prozesse und Systeme in Bezug auf die kontinuierliche Einhaltung der festgelegten Spezifikationen, sowie der Erhalt der Vollständigkeit, Richtigkeit, Unversehrtheit und Aktualität der Daten. Angemessene und regelmäßige Überwachung der Einhaltung, um Abweichungen festzustellen und anzupassen wo erforderlich. Neben der Fehlerfreiheit ist die Diskriminierungsfreiheit bei automatisierten Bewertungs- und Entscheidungsprozessen IM VORFELD zu prüfen, festzulegen und im Prozess sicher zu stellen.

Die rechtlichen Anforderungen ergeben sich aus der DS – GVO Art.5 Abs.1 lit.d, f, Art.32 Abs.1 lit.b (Integrität); Art.22 Abs.3,4 in Verbindung mit ErwGr.71 (Profiling, Fehler-, Diskriminierungsfreiheit); Art.32 Abs.1 lit.b (Belastbarkeit); Art.33 Abs.3 lit.d, Art.34 Abs.2 (Behebung und Abmilderung von Datenschutzverletzungen); Art.32, 33, 34 (Angemessene Überwachung der Verarbeitung)

>Praktisch:

Enge Eingrenzung von Lese- und Schreibrechten mittels Berechtigungskonzept. Einsatz von Prüfsummen, elektronischen Siegeln und Signaturen in Verarbeitungsprozessen gemäß eines Krypto - Konzeptes. „Härten" von IT – Systemen zur Vermeidung von Nebenfunktionalitäten. Dokumentiertes und angewendetes (Rollen-) Berechtigungskonzept. Prozesse zur Aufrechterhaltung der Aktualität, zum Löschen und zum Berichtigen von Daten und zur Identifizierung von Betroffenen. Durchführung von Tests zur Dokumentation und Feststellung der Funktionalität, von Sicherheitslücken, Risiken und Nebenwirkungen, einschließlich der Abläufe und Prozesse. Schutz vor äußeren Einflüssen und Zugriffen.

(d) Vertraulichkeit

>Systematisierung: Kein Zugriff, Kenntnisnahme oder Nutzung der Daten durch unbefugte Dritte, ob externe, Beschäftigte oder alle Arten von Dienstleistern. Dies gilt auch bei allen Arten von Zwischenfällen.

Die rechtlichen Anforderungen ergeben sich aus der DS – GVO Art.5 Abs.1 lit.f, Art.28 Abs.3 lit.b, Art.29, 32 Abs.1 lit.b, Art.32 Abs.4, Art.38 Abs.5 (Vertraulichkeit, Belastbarkeit); Art.33 Abs.3 lit.d, 34 Abs.2 (Behebung, Abmilderung von Schutzverletzungen)

>Praktisch:

Implementierung eines sicheren Authentifizierungsverfahrens. Festlegung und Kontrolle der Nutzung zugelassener Ressourcen, Kommunikationskanäle, Abläufe, interne Regelungen und vertragliche Verpflichtungen. Prozesse zur Verschlüsselung von Datentransfer und -speicherung, einschließlich der Sicherheit der Systeme und des entsprechenden Krypto – Konzeptes. Enge Eingrenzung des Berechtigungs- und Rollenkonzeptes auf nachprüfbar, identifiziertes und zulässiges Personal, dass örtlich, fachlich zuständig, befähigt, zuverlässig, ist, keinen Interessenkonflikten unterliegt und in angemessen ausgestatteten Räumlichkeiten arbeitet.

(e) Nichtverkettung

>Systematisierung: Die Vermeidung einer Zusammenführung / Verkettung von Daten, die zu unterschiedlichen Zwecken erhoben wurden ist durch technische und organisatorische Maßnehmen sicherzustellen (Pseudonymisierung, Anonymisierung, Berechtigungskonzepte). Eine rechtliche zulässige Verkettung ist nur unter eng definierten Umständen möglich.

Die rechtlichen Anforderungen ergeben sich aus der DS – GVO Art.5 Abs.1 lit.b (Zweckbindung)

>Praktisch:

Einschränkung von Verarbeitungs-, Nutzungs-, Transferrechten und Schnittstellen, incl. ausgefeiltem Rollen- und Berechtigungskonzept und nutzerkontrolliertem Identitätsmanagement. Trennung von Organisation und Abteilungsgrenzen. Qualitätssichernde Revision zur Compliance bei Software – Entwicklung und Verbot von Backdoors. Einsatz von Pseudonymisierung bzw. Anonymisierung und geregeltes Zweckänderungsverfahren.

(f) Transparenz

>Systematisierung: In unterschiedlichem Maße müssen Betroffene, Betreiber von Systemen und Kontrollinstanzen erkennen können, welche Daten wann, für welchen Zweck erhoben und verarbeitet werden, welche Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung in den einzelnen Phasen besitzt. Transparenz von der Entstehung bis zur Löschung.

Die rechtlichen Anforderungen ergeben sich aus der DS – GVO Art.5 Abs.1 lit.a, Art.12 Abs.1 und 3 bis Art. 15, Art. 34 (Transparenz für Betroffene); Art.5 Abs.2, Art.7 Abs.1, Art.24 Abs.1, Art.28 Abs.3 lit.a, Art.30, Art. 33 Abs. 5, Art. 35, Art. 58 Abs. 1 lit. a und lit. e (Rechenschafts- und Nachweispflicht); Art.32, 33, 34 (Angemessene Überwachung der Verarbeitung); Art.4 Abs.11, Art.7 Abs.4 (Einwilligungsmanagement)

>Praktisch:

Dokumentationskonzept im Sinne einer Inventarisierung und dem Zusammenspiel von Verarbeitungs-, Geschäftsprozessen, Datenbeständen, Datenflüssen, Netzplänen, IT – Systemen, Software, Betriebsabläufen, Profiling, Scoring, teilautomatisierten Entscheidungsprozessen, Zugriffen, Änderungen, Versionierungen, Überwachungen, Tests, Auswertungsanalysen, Datenschutz – Folgenabschätzungen bei geänderten oder neuen Prozessen sowie Verträge mit Mitarbeitern, Dritten und Auftragsverarbeitern. Dokumentation der Bearbeitung der Rechte von Betroffenen (Einwilligung, Widerruf, Widerspruch, Informationspflichten zu Erhebung, Quellen, Umfang, Benachrichtigungen bei Datenpannen, Zweckänderungen).

(g) Intervenierbarkeit

>Systematisierung: Erfüllung der den Betroffenen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Einschränkung, Übertragbarkeit, Widerspruch und Eingriff in automatisierte Bewertungs- und Entscheidungsprozesse, Profiling, sowie Maßnahmen zur Identifizierung bzw. Authentisierung. Zwecks Erfüllung der Betroffenenrechte und möglichen, behördlichen Anordnungen muss der Verantwortliche jederzeit Eingriff in die Prozesse nehmen können.

Die rechtlichen Anforderungen ergeben sich aus der DS – GVO Art.12 Abs. 2 (Wahrnehmung Betroffenenrechte), Art.12 Abs.6 (Identifizierung), Art.5 lit.d, Art.16 (Berichtigung), Art.17 Abs.1 (Löschung), Art.18 (Einschränkung), Art.20 Abs.1 (Übertragung), Art.22 Abs.3 (Eingriffsmöglichkeit Profiling), Art.25 Abs.2 (Datenschutz Voreinstellungen), Art.33 Abs.3 lit.d, Art.34 Abs.2 (Behebung, Abmilderungen bei Vorfällen), Art.4 Abs.11, Art.7 Abs.4 (Einwilligungsmanagement), Art.58 Abs.2 lit.f, j (aufsichtsbehördliche Anordnungen)

>Praktisch:

Differenzierte Einwilligungs-, Rücknahme -, Widerspruchsmöglichkeit durch notwendige, standardisierte Datenfelder (benachrichtigen, einwilligen, abrufen sperren, löschen, widersprechen, Gegendarstellung, Identifizierung, Authentifizierung), datenschutzfreundliche Voreinstellungen, ein „single point of contact“ für Betroffene. Dokumentation zur Bearbeitung von Anfragen, Störungen, Änderungen bei Verarbeitung und technisch – organisatorischen Maßnahmen.

Hier folgt in den nächsten Informationsbriefen nach und nach eine kurze Zusammenfassungen der einzelnen Inhalte. Im nächsten Informationsbrief „Teil 5“ Ziele als Design Strategie und Verzeichnis der Verarbeitungstätigkeiten.

(2) Zu Datenschutz

(a) EuGH Entscheidung (Juni)„kippt Datendeal mit USA“ ? !

Also eigentlich kein Problem, WENN neben dem grundsätzlichen Erlaubnis – Tatbestand die Speicherung und Verarbeitung der Daten in Europa oder einem Drittland das nach Prüfung der EU einen gleichgelagerten Datenschutz bietet (durch einen Angemessenheitsbeschluss der EU nach Art.45 der DS-GVO Link: EU - adequacy decisions). Die Zertifizierung von US – Unternehmen nach dem EU - US - Privacy - Shield - Abkommen (vorm. „Safe Haven“) ist nach dem Urteil nicht ausreichend u. a. durch den Zugriff von Strafverfolgungsbehörden und Geheimdiensten und fehlender Klagerechte.

Vorbehaltlich anderer Garantien können nach Art.46 der DS-GVO auch Daten an weitere Länder transferiert werden. Ein Punkt im Gesetz ist die Vereinbarung von durch die Aufsichtsbehörde genehmigter Standard – Datenschutz – Klauseln. Jedoch ist nach dem Urteil des EuGH die reine Vereinbarung nicht ausreichend, sondern im Vorfeld ist auch die Anwendbarkeit / Durchsetzbarkeit zu prüfen bzw. zu gewährleisten. Damit bleibt z. B. der US - „Behördenzugriff“ problematisch.

Eine Möglichkeit bleibt noch nach Art.49 DSGVO mit der Einwilligung des Betroffenen NACH eingehender Risikoaufklärung + Vertragserfüllung + im Interesse von Person, Unternehmen, Öffentlichkeit, oder + Verteidigung von Rechtsansprüchen, oder + Schutz lebenswichtiger Interessen, oder aus öffentlichem Register (Unionsrecht). Mehr Infos? Unter diesem LINK!

(b) Italien weist den Weg

Die Aufsichtsbehörde in Italien weist 2020 nach Deutschland 2019, wie ernst der Datenschutz in Europa genommen wird. Jli. 2020: 17,8 Mio. € an Wind Tre wegen intensiver Mail, Faxe, SMS und unerwünschte Telefonanrufe, Apps nur mit Einwilligung in Verarbeitungszwecke (wie Profiling u. ä.) Widerruf der Einwilligung erst nach 24 Stunden möglich. Jan. 2020: 8,5 Mio. € Bußgeld an ENI wegen unerwünschter Anrufe und „heimlicher Verträge". Jan. 2020: 27,8 Mio. € Bußgeld an TIM wegen aggressiver Telefonaktion sogar gegen Widerrufe.

(c) Und es trifft nicht nur die „Großen"!

229 € (Mrz. 2020) an LKW-Fahrer wegen Dashcam Nutzung und Youtube Veröffentlichung.
1.488 € (Jan. 2020) an Steuerberater wegen unzureichender Datenschutzmaßnahmen
20.000 € (Feb. 2020) HHVV wegen verspäteter Verstoß – Meldung an Betroffene und Aufsicht
830.000 € (Jli. 2020) BKR-NL wegen unerlaubt hoher Anforderungen an Auskunftsersuchen

In 2020 wurde bereits mehr als 200 Verstöße mit Geldbußen in allen Größenordnungen in Europa auf dem DSGVO – Portal erfasst. Interessant sind die jeweiligen Gründ Wer gerne in der Datenbank „stöbern" möchte, kann dies über den folgenden LINK – Datenbank Bußgelder mit Such- und Sortiermöglichkeiten in sehr übersichtlicher Form gern tun.

PS: Und wie in einem letzten Brief mitgeteilt, befinden sich die Behörden gerade erst im Aufbau von Personal, wozu die Staaten nach der Verordnung ja verpflichtet sind.

(3) Zu Datensicherheit

(a) PS: Zur EuGH Entscheidung für die Cloud:

Ich lese gerade für den Einsatz in einer Cloud, dass mit einer (Vor-) Verschlüsslung Dritten wie dem Cloud – Anbieter ja der Zugriff auf die Daten verwehrt. Zitat:

„Eine solche Verschlüsselung kann ebenfalls bewirken, dass das Datenschutzrecht von vornherein keine Anwendung findet und dementsprechend die „Übermittlung" auch nicht den Regelungen unterliegt. "

(b) Zeitlos wichtig: „Das Pizza-Passwort"

In einfacher, teils kurzweiliger Form gibt der BSI nach und nach Informationen zum 1x1 der IT – Sicherheit. Hier die LINKS im Juli: Passwörter | 2-Faktor-Sicherheit | Auto-Update |

(4) Zu angrenzenden Themen

(a) Echt jetzt?: "Bundesamt für Krisenschutz und Wirtschaftshilfe"

Post oder E-Mails vom "Bundesamt für Krisenschutz und Wirtschaftshilfe" oder gar vom "Bundesministerium zur Abwehr von Kriminalität im Cyberspace"?: VERGESSEN!!! Es ist alles eine Fälschung! Das BSI geht davon aus, dass es sich um mögliche Vorbereitungshandlungen für Straftaten wie Betrug oder Phishing handelt. Die Betrüger haben sogar Webseiten für die vermeintlichen Behörden entwickelt, welche zwischenzeitlich abgeschaltet sind, sodass von ihnen keine potenzielle Gefahr mehr ausgeht. LINK: BSI zu Phishing in Corona – Zeiten.

Juni 2020 | Zum Datenschutz aufgefallen

Information zum

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in),*

Aufsichtsbehörden sind im verpflichtendem Auf – und Ausbau, Verantwortliche wie Privatpersonen und auch Gerichte „*gewöhnen*“ sich langsam an die Pflichten und Rechte aus der EU – DS - GVO. Damit nehmen Neuigkeiten zum Datenschutz nicht ab. Hier finden sich die mir zum Datenschutz aktuell aufgefallenen Nachrichten.

Unter „Inhalt“ sind die Nachrichten übersichtlich aufgeführt. Mit einem Klick gelangen Sie zu einer kurzen Zusammenfassung mit Angabe von Quellen und Link. Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist.

Selbstverständlich können Sie sich auch bei diesen, wie bei allen Fragen zum Datenschutz gerne direkt an mich wenden.

Vielen Dank für Interesse

Inhalt

(zusammengestellt von Volker Schroer, zertifizierter Datenschutzbeauftragter)

(1) Serie: Standard-Datenschutzmodell („SDM“).....1

Teil 3: *Zentrale datenschutzrechtliche Anforderungen*.....1

(2) Zu Datenschutz.....2

a) Die Sache mit den Keksen!.2

b) WhatsApp ???.....2

(c) *Social Media Dienste! Dafür sind doch die Plattformen zuständig?*.....

i) Konstruktion rechtliche Grundlage (LDI - RP):.....3

ii) Datenschutzerklärung, ohne geht‘s nicht (Muster).....3

(d) Facebook – BGH bestätigt Bundeskartellamt.....3

(3) Zu Datensicherheit.....3

(a) 20 Jahre „I LOVE YOU“.....3

(4) Zu angrenzenden Themen.....3

(a) Die Corona – App ist da.....3

(1) Serie: Standard-Datenschutzmodell („SDM“)

Teil 3: Zentrale datenschutzrechtliche Anforderungen

Umfasst eine übersichtliche Aufzählung der gesetzlichen Anforderungen, nebst rechtlicher Ableitung und wo möglich, um die konkrete, praktische Sicht der Aufsicht dazu. Die Anforderungen sind (#Ergänzungen, sofern nicht aus dem Begriff schon hervorgehend):

Transparenz[1]	Zweckbindung[2]	Datenminimierung[3]
Richtigkeit	Speicherbegrenzung[3]	Integriät[4]
Vertraulichkeit	Berichtigungsmöglichkeit	Löschbarkeit
Rechenschaftspflicht / Nachweisfähigkeit	Identifizierung / Authentifizierung [5]	Unterstützung der Betroffenen bei der Ausübung der Rechte
Eingeschränkte Verarbeitung	Übertragbarkeit	Datenschutz-Voreinstellungen[6]
Eingriffsmöglichkeit bei automatisierter Entscheidung	Profiling: Fehler- und Diskriminierungsfreiheit	Behebung und Abmilderung von Schutzverletzungen
System - Verfügbarkeit	Belastbarkeit (Ausfallsicherheit)	Wiederherstellbarkeit
Evaluierbarkeit (Überprüfungen)	Angemessene Überwachung der Verarbeitung	
Einwilligungsmanagement[7]	Umsetzung aufsichtsbehördlicher Anordnungen	

[1])Spätestens nach einem Monat muss der Betroffene „so oder so“ über eine Verarbeitung informiert sein
[2])Angemessen = Zweck; Erheblich = notwendig zur Zweckerreichung; Beschränkt = kein „nice-to-have“ oder für „später“
[3])Speicherung nur das und solange es für den Zweck unbedingt erforderlich ist (Löschungspflicht! Auch Teile vorab)
[4]) Schutz vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung („TOM“)
[5])der Verantwortliche eine Vorgehensweise zur Authentifizierung von Personen, die die Betroffenenrechte geltend machen, festlegen und umsetzen muss.
[6])Minimale Voreinstellung von Einwilligungen, möglichst „optionale“ Erweiterungen (data protection by default)
[7])Konkrete, klare, eindeutige und umfassende Vorabinformation, gleiches zur Einwilligung / Zustimmung

Zusammenfassung der zentralen datenschutzrechtlichen Anforderungen in zwei Sätzen:

Wie in einer langfristigen Geschäfts - Beziehung ist das Gefühl von SICHERHEIT und VERTRAUEN die Basis und sollte sich in allen Punkten in einer offenen und fairen Zusammenarbeit wiederfinden, dann hat SIE auch langfristig Bestand. Für die Aufsicht sollte das „Gefühl" allerdings dokumentiert sein (Nachweispflicht).

Hier folgt in den nächsten Informationsbriefen nach und nach eine kurze Zusammenfassungen der einzelnen Inhalte. Im nächsten Informationsbrief „Teil 4: Systematisierung der Anforderungen durch die Gewährleistungsziele"

(2) Zu Datenschutz

(a) Die Sache mit den Keksen!

Ob Europäischer – Gerichtshof oder jetzt (28.05.2020) der Bundesgerichtshof unter Aktenzeichen (Pressemitteilung verlinkt): I ZR 7/16 - Cookie-Einwilligung II, MUSS konkrete, klare, eindeutige, umfassende leicht verständliche Vorabinformationen geben, um RECHTSWIRKSAM eine freiwillige und vom Nutzer verstandene Einwilligung / Zustimmung für das setzen von Cookies oder Telefonwerbung zu erhalten. Voreinstellungen, verschleiern oder verstecken ist unwirksam. Konkret:

- ✔ Cookies für die Steuerung von Funktionen und Präferenzen sind weiterhin ohne Einwilligung erlaubt, wenn sie sich auf eine Interessenabwägung gemäß Art. 6 Abs. 1 Buchst. f DSGVO stützen lassen. Denkbar sind Cookies für Spracheinstellungen, Schriften, Videoqualität, Chats u.s.w., sofern nicht mit Nutzerprofil verbunden, oder wenn sie unbedingt erforderlich sind, um dem Nutzer den gewünschten Dienst zur Verfügung zu stellen, z. B. Session-Cookies (Technik Warenkorb). Einzelfallentscheidung bleibt (noch)
- ✗ ***Werbung und Reichweiten Cookies dagegen bedürfen der ausdrücklichen Zustimmung.***

(b) WhatsApp ???

Privat („Haushaltsausnahme): ja. Für die geschäftliche Nutzung schwelen unverändert die Themen (- Schwerpunkte) mit dem Datenschutz zwischen Anbieter und Aufsicht:
- ✗ WhatsApp agiert außerhalb des europäischen Datenschutzbereiches
- ✗ Vertraulichkeit der Kommunikation wird in Frage gestellt
- ✗ Übertragung ALLER Kontaktdaten aus dem Adressbuch
- ✗ Backup über die Cloud

Nur unter bestimmten Voraussetzungen schreibt die Aufsicht als Fazit (LDI – RP) unter folgendem Link: https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/ kann der Dienst genutzt werden. Bei der Praktikabilität (Umsetzung, Anwendung) habe ich so meine Zweifel. Eine Übersicht zu Rechtsfragen bei Messengern mit Mustern hat das Rechenzentrum der Universität Würzburg veröffentlicht unter: https://www.rz.uni-wuerzburg.de/dienste/it-recht/it-vertraege/whatsapp/

(c) Social Media Dienste! Dafür sind doch die Plattformen zuständig?

DAS, kann man so leider nicht stehen lassen. Wie hier schon berichtet, sind die Aufsichtsbehörden der Ansicht, dass eine datenschutzkonformer Betrieb einer Fanpage am Beispiel Facebook (gilt auch für einige andere Social Media Dienste) nicht möglich ist. Der EuGH hielt im Juni 2018 eine gemeinsame, datenschutzrechtliche Verantwortung von Betreiber und Plattformanbieter fest, da es keine Verantwortungslücken im Datenschutz geben darf. Auch wenn keine direkte Einflussmöglichkeit des Betreibers auf die Verarbeitung des Anbieter gegeben ist. Das Bundesverwaltungsgericht stellt im September 2019 die Verantwortung und die Haftung des Fanpage – Betreibers bei Datenschutzverletzung gegenüber der Aufsicht heraus. ABER, auch die Aufsichtsbehörden haben erkannt, dass Social Media Dienste:

"... zu einem wesentlichen Bestandteil im beruflichen und privaten Informations- und Kommunikationsverhalten vieler Nutzerinnen und Nutzer geworden sind, bei dem die empfundenen Vorteile gegenüber bestehenden Datenschutzproblemen überwiegen ...",

Deshalb hat die Aufsichtsbehörde in Rheinland – Pfalz (LDI – RP) datiert mit 06.03.2020 einen (Verlinkt) „Handlungsrahmen für die Nutzung von Social Media durch öffentliche Stellen“ (mit „Vorbildcharakter“ für nicht – öffentliche Stellen), herausgegeben,

i) Konstruktion rechtliche Grundlage (LDI - RP):

Bei angemeldeten Nutzern kann die Einwilligung über die akzeptierten Nutzungsbedingungen des Plattformanbieters fingiert werden. Dies ist formalrechtlich zwar nicht restlos korrekt, da die Einwilligung nicht gleichzeitig gegenüber dem Seitenbetreiber erfolgte. Vorbehaltlich weiterer Erkenntnisse der Datenschutzkonferenz sei das aber akzeptabel. Voraussetzung hierfür ist aber in jedem Fall, dass die Nutzungsbedingungen der Plattform die Informationspflichten hinsichtlich der Verarbeitung der Nutzungsdaten erfüllen. (*Dies kann im Hinblick auf die abstrakte Nennung von verarbeiteten Daten und die offene Zweckbestimmung in den Nutzungsbedingungen einiger Anbieter durchaus bezweifelt werden.)*

ii) Datenschutzerklärung, ohne geht‘s nicht (Muster)

Facebook: https://volkerschroer.de/DSGVO/2020.06.30.Facebook.Hinweise.bei.Nutzung.Fanpages.pdf
Twitter: https://volkerschroer.de/DSGVO/2020.06.30.Twitter.Hinweise.bei.Nutzung.pdf

(d) Facebook – BGH bestätigt Bundeskartellamt

Datensammlung über Dienste hinweg und sogar bei Dritten nicht ohne Zustimmung !! Aber wie zu hören macht Facebook erst einmal weiter, da das Verfahren ja noch läuft (!?) LINK BGH-Presse

(3) Zu Datensicherheit

(a) 20 Jahre „I LOVE YOU“

Unter dem Titel (LINK): „Betreff: I LOVE YOU – klickst du noch oder löschst du schon?“ hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) unter dem 4. Mai 2020 auf die immer noch weit verbreitete Gefahr der Verbreitung von Schadsoftware über E – Mails hingewiesen. Laut SECURITY Cyberdefense & ID Protection Conference 2020 erfolgen weit über 90% der Cyberangriffe auf Unternehmen durch das Einfallstor E-Mail-Anhang. Über getarnt als Dateianhang einer nur scheinbar vertrauenswürdigen E-Mail, als versteckte "Zugabe" bei einem Gratis-Download, durch bösartige Makros innerhalb eines Office-Dokuments (nur nach Aktivierung) oder präparierte Werbebanner auf Webseiten. Wesentliche, vorbeugende Maßnahmen sind:

Schulung	Systemeinstellung und Updates	Backup und Notfallprozess
 4 min. Video Online Sicherheit		4 min. Video Netzwerk, System und Software schützen

Der 3x3 (Fragen & Sekunden) Sicherheitscheck des BSI:

- ✔ Kenne ich den Absender, ist die Adresse korrekt?
- ✔ Ist der Betreff sinnvoll und stimmig?
- ✔ Erwarte ich einen Anhang?
- ✗ Nicht? Beim Absender nachfragen oder gleich löschen!

Weitere Information und Hinweise in dem oben verlinkten Artikel des BSI.

(4) Zu angrenzenden Themen

(a) Die Corona – App ist da

Zu der Corona – App sind viele, sehr viele Informationen im Netz und in den Medien, sodass ich Sie hier nicht „strapazieren“ möchte. Zwei heiß diskutierte Themen sind mir aufgefallen:

- Chaos Computer Club lobt deutsche Corona-App (Link ZDF) Zitat: „*Es ist der vielleicht größte Ritterschlag, den die Corona-App, die heute startet, bekommen könnte: Der Chaos Computer Club empfiehlt sie zwar nicht. Aber: Er meckert auch nicht.*“ …. deshalb habe ich sie mir heruntergeladen.
- Vieles ist rechtlich noch unklar (Link Artikel Haufe), weshalb viele auch ein Gesetz zur Freiwilligkeit fordern, was ja allen Nutzern von der Bundesregierung zugesagt ist. Das bezieht sich nicht nur auf Arbeitsrecht, auch bei Besuchen von Geschäften und Restaurants sind sich die Juristen nicht „wirklich“ einig bei der Auslegung und wir sind gespannt!

Mai 2020 | Zum Datenschutz aufgefallen

Information zum

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in),*

Aufsichtsbehörden sind im verpflichtendem Auf – und Ausbau, Verantwortliche wie Privatpersonen und auch Gerichte *„gewöhnen“* sich langsam an die Pflichten und Rechte aus der EU - DSGVO. Damit nehmen Neuigkeiten zum Datenschutz nicht ab. Hier finden sich die mir zum Datenschutz aktuell aufgefallen Nachrichten.

Unter „Inhalt“ sind die Nachrichten übersichtlich aufgeführt. Mit einem Klick gelangen Sie zu einer kurzen Zusammenfassung mit Angabe der Quellen und Link. Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist.

Selbstverständlich können Sie sich auch bei diesen, wie bei allen Fragen zum Datenschutz gerne direkt an mich wenden.

Vielen Dank für Interesse

Inhalt

(zusammengestellt von Volker Schroer, zertifizierter Datenschutzbeauftragter)

(1) Serie: Standard-Datenschutzmodell („SDM“).....1

Teil 2: Einleitung & Ziele.....1

(2) Zu Datenschutz.....2

(a) Wie könnte eine Datenschutzrichtlinie aussehen?.....2

(b) Ist Datenschutz gleich Datensicherheit?.....2

(c) Einladung zum Online-Meeting einfach so?.....2

(d) Datenschutz in „Corona“ – Zeiten.....2

(3) Zu Datensicherheit.....3

(a) KoViKo - Kompendium Videokonferenzsysteme.....3

(b) ZOOM 5.0.....3

(c) Jitsi Meet – Empfelungen für die Severeinstellungen.....3

(d) iOS-App Mail „kritisch“ eingestuft.....3

(4) Zu angrenzenden Themen.....3

(a) Die Bundesaufsicht zieht um! Warum?.....3

(b) Cyber-Kriminelle lieben alte Software.....3

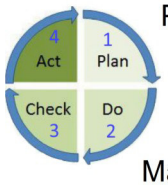
(1) Serie: Standard-Datenschutzmodell („SDM“)

Teil 2: Einleitung & Ziele

Ziel ist die Überführung der rechtlichen Anforderungen (Gewährleistungsziele der DS-GVO) zu den technischen und organisatorischen Maßnahmen in einen detaillierten **Referenzmaßnahmenkatalog für *den praktischen, täglichen Gebrauch des Verantwortlichen*** mit der Möglichkeit eines systematischen, nachvollziehbaren SOLL | IST Vergleichs (Prüfungskriterien!).

(1) Zweck: Das SDM dient ausschließlich einer datenschutzrechtlich konformen Gestaltung von Verarbeitungstätigkeiten nach dem Datenschutzrecht (Transformationshilfe: Recht zu Praxis).

(2) Anwendung & Struktur: Systematisierende, rollierende (Vor-) Planung, Einführung, Betrieb, Prüfung und Beurteilung der verwirklichten und zu verwirklichenden Geschäfts- und Verarbeitungsprozesse, einschließlich mit personenbezogenen Daten. Die DS-GVO verlangt ein nachweisbares Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (TOMs).



(3) Sieben Gewährleistungsziele *„von elementarer Bedeutung“* (aus Sicht des Betroffenen)

1.) Verfügbarkeit; 2.) Integrität; 3.) Datenminimierung; 4.) Vertraulichkeit;
5.) Nichtverkettung; 6.) Transparenz; 7.) Intervenierbarkeit.

In zwei Sätzen würde ich Einleitung und Ziele des SDM wie folgt zusammenfassen:

> ***Ein (rollierender, systematischer) Plan, auch Datenschutzrichtlinie genannt und die laufende Dokumentation dessen Einhaltung vermeidet „Ärgernisse“ für den Verantwortlichen und das Unternehmen. Es ist weniger Aufwand als es auf den ersten Blick scheint – wenn man es macht!***

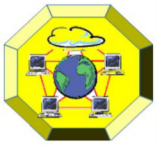
Hier folgt in den nächsten Informationsbriefen nach und nach eine kurze Zusammenfassungen der einzelnen Inhalte. Im nächsten Informationsbrief „Teil 3: Zentrale Anforderungen“

(2) Zu Datenschutz

(a) Wie könnte eine Datenschutzrichtlinie aussehen?

Die Datenschutzrichtlinie ist eine zentrale Aussage der Geschäftsleitung zum Daten – Schutz – Management (– System) im Unternehmen und dient den handelnden Mitarbeitern als Anleitung für das Tagesgeschäft. Natürlich dient sie auch der Rechenschaftspflicht gegenüber der Aufsicht. Der Umfang hängt sicherlich von verschiedensten Faktoren wie Sensibilität, Quantität und der Datenverarbeitungsarten, Unternehmensgröße, Branche u. ä. ab. Wenn zu technischen und / oder organisatorischen Maßnahmen bereits Richtlinien bestehen kann auch auf diese verwiesen werden. Wie in Art.12 Abs.1 lit.1 festgehalten sollte die Richtlinie präzise, transparent, verständlich, in leicht zugänglicher Form, sowie in klarer und einfacher Sprache verfasst sein. Damit ist ein beschränkter Umfang (von erfahrungsgemäß zwischen 5 bis 15 Seiten) wünschenswert. Eine von mir erstellte Entwurfsvorlage finden Sie unter folgendem LINK

(b) Ist Datenschutz gleich Datensicherheit?

Datenschutz	Datensicherheit
 Schutz der Daten, die sich auf **Personen** beziehen und Einhaltung der Fristen und Rechte wie Einwilligung, Auskunft, Löschung usw.	Schutz aller Systeme & Daten zur Gewährleistung der Integrität, Vertraulichkeit und jederzeitigen Verfügbarkeit 
 Ein dritter Baustein ist der **Unternehmens**datenschutz (Wirtschaftsspionage und - betrug) mit dem Geschäfts – Geheimnis - Gesetz (LINK zu GeschGehG)	Natürlich gibt es eine Schnittmenge dort, wo es neben den gesetzlichen Anforderungen um technisch - organisatorische Maßnahmen („TOM“) zum Schutz der Personendaten und Unternehmensdaten geht.

(c) Einladung zum Online-Meeting einfach so?

So einfach geht es nicht (war klar!). Da auch hier personenbezogene Daten verarbeitet werden, muss der Nutzer (Betroffene) informiert werden. Zum einen gleich mit einem kurzen Hinweistext in der Einladung mit Verweis auf eine Datenschutz(auf)erklärung. Die kann standardmäßig hinterlegt sein oder als Dokument angehängt werden. Hier nachfolgende Muster / Anwendungshinweise:
BLIZZ: https://volkerschroer.de/DSGVO/2020.05.31.BLIZZ.Hinweis.bei.Verwendung.pdf
Jitsi Meet: https://volkerschroer.de/DSGVO/2020.05.31.Jitsi.Meet.Hinweis.bei.Verwendung.pdf
MS Teams: https://volkerschroer.de/DSGVO/2020.05.31.MSTeams.Hinweis.bei.Verwendung.pdf
ZOOM: https://volkerschroer.de/DSGVO/2020.05.31.ZOOM.Hinweis.bei.Verwendung.pdf

(d) Datenschutz in „Corona“ – Zeiten

Der „Aufreger“ ging ja durch alle Medien. Im Zuge der Pandemie müssen in vielen Geschäften und der Gastronomie unser Kontaktdaten hinterlegt werden. Eine offene Liste, an der ich erkennen kann, wer während und vor mir dort ist und war ist sicherlich nicht datenschutzkonform. Die Aufsichtsbehörde (LDI) in NRW hat dazu Hinweise unter folgendem LINK veröffentlicht.

- Rechtmäßigkeit der Erhebung ist die gesetzliche Vorgabe der Corona Schutzverordnung NRW bzw. des jeweiliges Bundeslandes. Eine zusätzliche Einwilligung ist immer gut.
- Erhebungsdaten sind: Name, Adresse, Telefonnummer Zeitpunkte des Betretens und Verlassens.
- Speicher-, Aufbewahrungs- bzw. Löschfrist: 3 Wochen.
- Übermittlung ausschließlich an das jeweilige Gesundheitsamt nach Aufforderung.
- Informationspflicht (Datenschutzerklärung): Muster (docx) der Aufsicht unter folgendem LINK
  PS: Steht zwar für Niedersachsen in der Fußnote gilt aber auch für NRW und wäre zu ändern!

Zur Form der Erfassung sowie zur Prüfung der Daten kann ich keine Ausführungen (Vorschriften) bisher finden, sodass für einer Erfassung noch alle Freiheiten (z. B. Portal, elektronisch – über

einen QR-Code Aufruf, Smartphone) gegeben sind. Weitere Informationen gibt es auch bei „a.s.k. Datenschutz e. K. mit verschiedenen Mustern unter folgendem LINK

(3) Zu Datensicherheit

(a) KoViKo - Kompendium Videokonferenzsysteme

Die Aufsichtsbehörde für die Datensicherheit, das Bundesamt für die Sicherheit in der Informationstechnik (BSI) hat ein Kompendium für Videokonferenzsysteme aufgelegt und schreibt dazu:

„Das Kompendium Videokonferenzsysteme (KoViKo) richtet sich an Entscheider, Planer, Beschaffer, Betreiber, Administratoren, Auditoren und auch Endnutzer, die über Videokonferenz Inhalte beziehungsweise Informationen mit normalem und erhöhtem Schutzbedarf austauschen. Das vorliegende Dokument betrachtet nicht den Einsatz einer Videokonferenzlösung in Arbeitsbereichen mit Verschlusssachen (VS-Bereichen).“

Wer die 173 Seiten lesen möchte oder muß, findet diese über folgenden LINK.

(b) ZOOM 5.0

Hinsichtlich der Sicherheit war „ZOOM“ im März etwas ins Kreuzfeuer geraten. Worauf man eine 90 – Tage – Fokus - Initiative - Sicherheit gestartet hat. Bei dem jetzt veröffentlichtem „Zoom 5.0“ hat der Anbieter an zahlreichen Stellrädchen gedreht und dabei auch Passwortvorgaben und Standardeinstellungen angepasst. Die wesentlichen Änderungen in der Sicherheit hat CloudComputing-Insider zusammengestellt. Diese finden Sie unter folgendem LINK.

(c) Jitsi Meet – Empfelungen für die Severeinstellungen

Die Konferenzanwendung ist als quelloffenes Open – Source Projekt auch auf eigenen Server installierbar. Da ich Datenschutz- und nicht Datensicherheitsbeauftragter bin, wurde mir für eine datenschutzfreundliche Nutzung die Seite von „KUKETZ ITSecurtiy“ für die Servereinstellung unter folgendem LINK empfohlen.

(d) iOS-App Mail „kritisch“ eingestuft

Ein weiterer „Aufreger“ ist das Mail – Programm von Appel. Wie das BSI in seiner Pressemitteilung vom 23.4. schreibt, ist eine als "sehr kritisch" eingestufte Sicherheitslücke in der iOS-App "Mail" aufgetaucht. Aber das BSI bietet auch eine Lösung für den Schutz der E – Mails und Geräte. Die einfache Variante = deaktivieren / löschen und anderen Client oder Webmail benutzten. Zumindest sollte die Hintergrundsynchronisation deaktiviert werden. Details unter folgendem LINK

(4) Zu angrenzenden Themen

(a) Die Bundesaufsicht zieht um! Warum?

{Der BfDI informiert} Die Behörde des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zieht zum 18. Mai 2020 in ein neues Gebäude. Vor allem durch den personellen Zuwachs der letzten Jahre mussten neue Räumlichkeiten gefunden werden. Nach Art.52 DS-GVO hat jedes Mitgliedsland jetzt unter anderem „… für eine personell, technisch und finanziell angemessene Ausstattung zu sorgen.“ (!!!) Sie ist noch nicht am Ziel. (Presselink) und *„Die neue Liegenschaft bietet Raum für weiteren Personalaufwuchs beim BfDI.“* (Presselink)

(b) Cyber-Kriminelle lieben alte Software

Im seinem [Buerger-Cert-Newsletter] vom 28.05.2020 schreibt das Bundesamt für Sicherheit in der Informationstechnik „recht süffisant“:

„Auch Hacker mögen es gerne bequem: Um sich unnötige Arbeit mit dem Ausspionieren moderner Systeme zu sparen, versuchen sie oft, bekannte alte und ungepatchte Lücken auszunutzen. Das geht aus einem Bericht der Cybersecurity and Infrastructure Security Agency (CISA), dem Federal Bureau of Investigation (FBI) und der US-Regierung hervor, meldet Heise Online.“

Zum Artikel Heise Online gelangen Sie über folgenden LINK.

PS: Die anderen Überschriften waren auch nicht „langweilig“ wie:

Cyber-Kriminelle verschaffen sich Zugang zu Kundendaten von Easyjet || Nach Cyber-Angriff: Ruhr-Universität Bochum ruft zu Passwortänderungen auf || Daten des Hasso – Plattner - Instituts für Unbefugte einsehbar || Bundesagentur für Arbeit: Schadsoftware statt Stellenangebote

April 2020 | Zum Datenschutz aufgefallen

Information zum

Datenschutz - Service

oder Fragen per Mail an:

Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtig- und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in),*

Aufsichtsbehörden sind im verpflichtendem Auf – und Ausbau, Verantwortliche wie Privatpersonen und auch Gerichte „*gewöhnen*“ sich langsam an die Pflichten und Rechte aus der EU - DSGVO. Damit nehmen Neuigkeiten zum Datenschutz nicht ab. Hier finden sich die mir zum Datenschutz aktuell aufgefallen Nachrichten.

Unter „Inhalt“ sind die Nachrichten übersichtlich aufgeführt. Mit einem Klick gelangen Sie zu einer kurzen Zusammenfassung mit Angabe der Quellen und Link. Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist.

Selbstverständlich können Sie sich auch bei diesen, wie bei allen Fragen zum Datenschutz gerne direkt an mich wenden.

Vielen Dank für Interesse

Inhalt

(zusammengestellt von Volker Schroer, zertifizierter Datenschutzbeauftragter)

(1) Serie: Standard-Datenschutzmodell („SDM“).....1

Teil 1: Wer und Warum.....1

(2) Zu Datenschutz.....2

(a) Datenschutzregelung im Home – Office.....2

(b) 9. Tätigkeitsbericht 2020 des BayLfD.....2

i) Facebook Fanpages nicht DSGVO konform.....2

ii) Einsatz von Tracking–Tools 2

iii) Google Analytics nur mit Einwilligung.....2

iv) IST Windows 10 Datenschutzkonform? Die Aufsicht prüft!.....2

v) Werbung per E – Mail / SMS, B2C wie B2B.....2

vi) Background Screening von Bewerbern?.....2

vii) Reicht die Information bei der Mitgliederverwaltung in Vereinen?.....2

viii) Rapider Anstieg von Datenschutzverletzung 2020..3

ix) Bußgeldgründe in Bayern..3

(c) Bußgeldverfahren und -festsetzung, wie läuft das.....3

(3) Zu Datensicherheit.....3

(a) „Up-to-date“??? Anstieg von Sicherheitslücken.....3

(4) Zu angrenzenden Themen.....3

(a) Erste-Hilfe-Kit bei verteiltem Arbeiten.....3

(b) Digitales Lernen: Sicherheitstipps für Eltern.....3

(1) Serie: Standard-Datenschutzmodell („SDM“)

***Entscheidung und damit Risiken und Haftung tragen ausschließlich die Verantwortlichen**, i. d. R. die Geschäftsleitung. Zu den Aufgaben des Datenschutzbeauftragten als Unterstützung für die Verantwortlichen, gehört die Information, Beratung, Sensibilisierung, Prüfung, Schulung der Verantwortlichen und Mitarbeiter und dient als Anlaufstelle für Betroffene und Aufsichtsbehörden.*

Teil 1: Wer und Warum

Die *Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (kurz: „DSK“ = Datenschutzkonferenz)* hat zur „praktischen, täglichen“ Unterstützung der Verantwortlichen bei der Einhaltung der gesetzlichen Regelungen ein ***Standard-Datenschutz-Modell*** entwickelt, in der aktuellen Version 2.0a vom 06.11.2019. Auf 69 Seiten als „Werkzeug“ für Verantwortliche konzipiert, ist es im Fall der Fälle die Prüfungsanforderung der Aufsicht. In zwei Sätzen würde ich es wie folgt zusammenfassen:

Schützen Sie Ihre Daten wie Ihre Liquidität und ganz besonders die von Ihren Kunden und Dritten. Mit der richtigen und kontinuierlichen Dokumentation dazu, vermeiden Sie Risiken, reduzieren Kosten und schonen die Liquidität.

Hier folgt in den nächsten Informationsbriefen nach und nach eine kurze Zusammenfassungen der einzelnen Inhalte. Es folgt im nächsten Informationsbrief „*Teil 2: Einleitung & Ziele*“

(2) Zu Datenschutz

(a) Datenschutzregelung im Home – Office

Die Datenschutzregeln machen vor dem Home – Office nicht halt und sollten, wenn nicht schon geschehen, geregelt werden. Einen Entwurfsvorschlag für die Richtlinie finden Sie hier [PDF]. Mit dem §7 Ausnahmen, können Sie die Regelungen um Besonderheiten zur aktuellen Situation, z. B. Lieferverzögerung bei (Firmen) Hardware oder räumliche Sondersituationen mit (befristeten) Regelungen ergänzen.

(b) 9. Tätigkeitsbericht 2020 des BayLfD

Aus dem 9. Tätigkeitsbericht für 2019 des Bayrischen Landesamtes für Datenschutz (Seiten) https://www.lda.bayern.de/media/baylda_report_09.pdf

i) Facebook Fanpages nicht DSGVO konform

{BLfD Tätigkeitsbericht 2019 S. 29} Betreiber von Facebook Fanpages haben nach derzeitigem Stand keine Möglichkeit, diese datenschutzkonform zu betreiben und müssen deshalb damit rechnen, Adressat von Anordnungen der Aufsichtsbehörden zu werden.

ii) Einsatz von Tracking–Tools

{BLfD Tätigkeitsbericht 2019 S. 29/30} Die Datenschutzkonferenz hat zum Einsatz von Tracking - Tools eine „Orientierungshilfe Telemedien“ veröffentlicht. Wichtig für Website - Betreiber ist, dass *nicht jeder Einsatz von Cookies einwilligungsbedürftig* ist, es nicht auf den Einsatz von Cookies ankommt, *sondern* sich die datenschutzrechtlichen Anforderungen immer *an der Verarbeitungs-tätigkeit orientieren* und die Voraussetzungen des Art. 6 Abs. 1 Buchst. f DS-GVO anhand einer dreistufigen Prüfung zu ermitteln sind. ***Der alleinige Hinweis, Direktwerbung sei ein berechtigtes Interesse, reicht nicht aus***.Außerdem erhalten Website-Betreiber wichtige Hinweise zur datenschutzkonformen Gestaltung eines sog. „Cookie-Banners“. Die dort genannten Anforderungen gelten für den Fall, dass eine Einwilligung des Nutzers eingeholt werden muss.

iii) Google Analytics nur mit Einwilligung

{BLfD *Pressemitteilung*} Dienste zur statistischen Analyse von Besuchern einer Webseite werden von vielen Webseitenbetreibern eingesetzt. Bei mancher dieser Produkte wie z.B. Google Analytics werden personenbezogene Daten Teil eines umfassenden Internetprofils (Tracking). Dann *muss eine Einwilligung* von den Besuchern *eingeholt werden*.

iv) IST Windows 10 Datenschutzkonform? Die Aufsicht prüft!

{BLfD Tätigkeitsbericht 2019 S.22} Die unabhängige Fachgruppe der Datenschutzkonferenz (DSK) hat sich im Dezember 2019 zu einer Laboranalyse von Windows 10 entschieden und durchgeführt. Sollte sich das Ergebnis beim realen Einsatz von Windows 10 bestätigen, dann stellt zumindest der Umgang mit Telemetriedaten bei Windows 10 Enterprise keinen datenschutzrechtlichen Hinderungsgrund dar. Der Einsatz von Windows 10 Pro könnte möglicherweise ein weiterer Arbeitsauftrag der Datenschutzkonferenz (DSK) werden.

v) Werbung per E – Mail / SMS, B2C wie B2B

{BLfD Tätigkeitsbericht 2019 S. 37/38} Werbung per E-Mail oder SMS kann *bei Bestandskunden* auf Basis eines berechtigten Interesses nach Art. 6 Abs. 1 Buchst f DS-GVO erfolgen, *ansonsten nur mit Einwilligung* der betroffenen Personen.

vi) Background Screening von Bewerbern?

{BLfD Tätigkeitsbericht 2019 S. 47} Potentielle Arbeitgeber dürfen sich nicht bei Facebook über Bewerber informieren.

vii) Reicht die Information bei der Mitgliederverwaltung in Vereinen?

{BLfD Tätigkeitsbericht 2019 S. 52} Rechtsgrundlage für die Verarbeitung personenbezogener Daten zum Zwecke der Mitgliederverwaltung im Verein ist Art. 6 Abs. 1 Buchst. b DS-GVO. Eine Einwilligung wird für diesen Verarbeitungszweck jedoch grundsätzlich nicht benötigt. Auch ein „Bestätigen lassen“ des Erhalts der nach Art. 13 DS-GVO zu erteilenden Informationen durch Unterschrift ist nicht erforderlich. Jedoch muss der Verein in der Lage sein, im Rahmen der

Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) nachzuweisen, dass er die nach Art. 13 DS-GVO zu erteilenden Informationen zur Verfügung gestellt hat. Dieser Nachweis kann unkompliziert z.B. durch Information auf dem (vom Neumitglied ausgefüllten) Formular enthalten sein, mit dem die Mitgliedschaft beantragt wird.

viii) Rapider Anstieg von Datenschutzverletzung 2020

{BLfD Tätigkeitsbericht 2019 S. 52} Mit der DS-GVO stieg die Anzahl der Meldungen nach Art. 33 DS-GVO rapide an und blieb bis zum Ende des Berichtsjahres auf einem hohen Niveau bestehen.

ix) Bußgeldgründe in Bayern

{BLfD Tätigkeitsbericht 2019 S. 71} Nach wie vor erreicht die Behörde viele Fälle, die den Einsatz von Dash-Cams, Videoüberwachung des öffentlichen Raums durch Private oder Veröffentlichungen personenbezogener Daten im Internet ohne Einwilligung der Betroffenen – v.a. auf Social - Media Plattformen wie Facebook, Instagram und WhatsApp – betreffen. Insgesamt wurden ca. 100 Bußgeldverfahren abgeschlossen. PS: „Die Aufsichtsbehörden in allen Bundesländern stocke kontinuierlich auf.

(c) Bußgeldverfahren und -festsetzung, wie läuft das

{Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen} Die Bußgeld - Zumessung erfolgt gegen Unternehmen in fünf Schritten. Zunächst wird das betroffene Unternehmen einer Größenklasse zugeordnet (1.), danach wird der mittlere Jahresumsatz der jeweiligen Untergruppe der Größenklasse bestimmt (2.), dann ein wirtschaftlicher Grundwert ermittelt (3.), dieser Grundwert mittels eines von der Schwere der Tatumstände abhängigen Faktors multipliziert (4.)und abschließend der unter 4. ermittelte Wert anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände angepasst (5.) Mehr: Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen

(3) Zu Datensicherheit

(a) „Up-to-date“??? Anstieg von Sicherheitslücken

{BSI} Meldet im April verstärkte Angriffe und Sicherheitslücken auf Betriebssysteme Windows, Apple, Linux (Serversysteme) sowie alle Browser. Warnung vor Apples Mail-App. Mehr: CERT-BUND-Meldungen.

{t3n} Zwei Sicherheitslücken im WordPress-Plugin Rank Math (200.000 Websites betroffen) Die Lücken seien am 26. März mit Version 1.0.41.1 geschlossen worden; Nutzer habe man via E-Mail benachrichtigt. Mehr: https://t3n.de/news/sicherheitsluecken-rank-math-1267730/

(4) Zu angrenzenden Themen

(a) Erste-Hilfe-Kit bei verteiltem Arbeiten

{UIG e.V. / Karlsruher Institut für Technologie} Social Distancing hat dazu geführt, dass beinahe jedes Unternehmen einen Großteil der Arbeit verteilt und vom Home - Office heraus erledigen muss. Für viele Unternehmen kommt das unerwartet und erzeugt Komplikationen. Zu diesem Zweck hat das Kompetenzzentrum Mittelstand 4.0 gemeinsam mit dem Karlsruher Institut für Technologie einen einfachen und verständlichen Erste-Hilfe-Kit erstellt. Mehr: https://www.kompetenzzentrum-usability.digital/angebote/demonstratoren/social-distancing-social-awareness/erste-hilfe-kit-fuer-erfolgreiches-verteiltes-arbeiten

(b) Digitales Lernen: Sicherheitstipps für Eltern

{Buerger – Cert – Newsletter 02.04.2020} Weil Kitas und Schulen geschlossen sind, nutzen Kinder und Jugendliche vermehrt digitale Dienste auf dem Tablet, Smartphone oder PC. Das freut nicht nur die Jüngsten, sondern auch ihre Eltern, weil es für sie eine Entlastung darstellt. Doch sollten dabei ein paar Sicherheitshinweise wie das Einschränken der App-Berechtigungen sowie Verhaltenstipps berücksichtigt und gerade Kinder beim digitalen Lernen und Spielen begleitet werden. Mehr: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/tipps-fuer-eltern-sicher-digital-lernen.html

Nachrichtenfetzen | Datenschutz | 2020 März

Interim Projekte & Management
Treasury | Finanzen | Datenschutz
Tel: +49 151 2756 3805
E-Mail: Mail2@volkerschroer.de
Webadresse: www.volkerschroer.de
Sitz: Essen / DE
XING: www.xing.com/profile/Volker_Schroer/cv

Inhalt

(1) Zu Datenschutz 1
(a) DSK gibt Hinweise zu Datenschutz und Corona {*BfDI Pressemitteilung*} 1
(b) Ein Datenleck melden - wie geht das? *{boxcryptor-Blog}* 2
(c) Was ist Auftragsverarbeitung nach DSGVO und was nicht? {*Security-Insider*} 2
(d) Kann ich Zoom-Video-Calls auch DSGVO-konform durchführen? {anwalt.de / datenschutz-guru.de} 2
(e) Videoüberwachung, insbesondere von Beschäftigten (Beispiele) {*Security-Insider*} 2
(f) Personalanalyse – wie weit darf der Arbeitgeber gehen? {*IT-Business*} 2
(g) E-Privacy-Verordnung: Es tut sich etwas an der Cookie-Front {*IT-Business*} 2
(h) Löschkonzepte nach der DSGVO {*IT-Business*} 3
(i) Geschäftliche E-Mails: Signatur, Impressum und DSGVO-Pflichtangaben {*eRecht24*} 3
(j) E-Mails an Warenkorb-Abbrecher: Sind sie rechtlich zulässig? {*eRecht24*} 3
(k) Bildrechte: So nutzen Sie Bilder rechtssicher auf Webseiten und Blogs {*eRecht24*} 3
(l) Ulrich Kleber – BfDI: Weitergabe Telekom-Standortdaten datenschutzrechtlich vertretbar 3
(2) Zu Datensicherheit („TOM“) 3
(a) Tipps für sicheres mobiles Arbeiten. Arbeiten von zu Hause oder unterwegs {BSI} 3
(b) Coronavirus: Homeoffice: Technik, Sicherheit, Fallstricke {*IT-Business*} 4
(c) Cloud-Apps benötigen mehr als nur Passwortschutz {Cloud-Computing-Insider} 4
(d) Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.1 {BSI} 4
(e) Zielscheibe: „Mensch“ So schützen sich Unternehmen {Security-Insider} 4
(f) Gesetzeslage und Anforderungen an IT-Sicherheit in der Zukunft {*IT-Business*} 4
(g) Neue Sicherheitsrisiken durch Sprachassistenten {*IT-Business*} 4
(h) Angreifer können WPA2 hacken {*Security-Insider*} 5
(3) Zu übergreifenden Themen 5
(a) Home Office: Was Unternehmer und Mitarbeiter zu Datenschutz und Arbeitsrecht beachten müssen {*eRecht24*} 5
(b) Gut 40 Prozent deutscher Unternehmen erleben Cyberangriffe {*IT-Business*} 5
(c) Psychisches Hacking der „Schwachstelle Mensch“ {Security-Insider} 5
(d) Coronavirus macht Homeoffice zum Hacker-Ziel {Security-Insider} 5

(1) Zu Datenschutz

(a) *DSK gibt Hinweise zu Datenschutz und Corona {BfDI Pressemitteilung}*

Die Datenschutzkonferenz (DSK), das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, veröffentlicht Informationen für Arbeitgeber und Dienstherren zum Umgang mit dem Datenschutz im Zusammenhang mit der Corona-Pandemie. Die Datenschützer stellen klar, dass der Schutz personenbezogener Daten und Maßnahmen zur Bekämpfung der Infektion sich nicht entgegenstehen. Die ausführlichen Hinweise zum Umgang mit dem Datenschutz während der Corona-Pandemie finden Sie auf der Internetseite des BfDI.

Artikel auf www.bfdi.bund.de

(b) *Ein Datenleck melden - wie geht das? {boxcryptor-Blog}*
Was tun, wenn es im Unternehmen zu einem Datenschutzvorfall kommt? Der Artikel gibt einen Überblick zu aktuellen Vorgaben nach der DS-GVO und nennt vorbeugende technische und organisatorische Maßnahmen, die Sie in ihrem Unternehmen sofort umsetzen können.
Weiterlesen: https://www.boxcryptor.com/de/blog/post/data-breach-report-how-to/?utm_medium=post&utm_source=newsletter&utm_campaign=de.newsletter.b2b.lead.databreach&utm_content=blogpost.databreach

(c) *Was ist Auftragsverarbeitung nach DSGVO und was nicht? {Security-Insider}*
Die Aufsichtsbehörden für den Datenschutz berichten, dass Unternehmen Schwierigkeiten damit haben, eine Datenverarbeitung als Auftragsverarbeitung einzustufen und entsprechend die passenden Datenschutz-Maßnahmen zu ergreifen. Wir berichten von konkreten Beispielen, beschreiben die Positionen der Aufsichtsbehörden und geben Tipps, wie man eine Auftragsverarbeitung erkennt.
Weiterlesen: **https://www.security-insider.de/was-ist-auftragsverarbeitung-nach-dsgvo-und-was-nicht-a-907849/?cmp=nl-36&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501**

(d) *Kann ich Zoom-Video-Calls auch DSGVO-konform durchführen? {anwalt.de / datenschutz-guru.de}*
Meldungen über Datenschutzprobleme die behebbar sind, unter anderem Deaktivierung des „Aufmerksamkeitstrackings“. ZOOM entfernt „Facebook-Tracker“. Einhaltung der DS-GVO und Auftragsverarbeitungsvertrag nach DSGVO
Weiterlesen: https://www.anwalt.de/rechtstipps/kann-ich-zoom-video-calls-auch-dsgvo-konform-durchfuehren_165202.html
& https://www.datenschutz-guru.de/datenschutz-tipps-6-2020-muster-anleitungen-co-fuer-online-meetings-via-zoom/
EU-DSGVO: https://support.zoom.us/hc/en-us/articles/360000789323-Data-Processing-Addendum

(e) *Videoüberwachung, insbesondere von Beschäftigten (Beispiele) {Security-Insider}*
Beschwerden, die Videoüberwachung zum Gegenstand haben, nehmen quantitativ seit Jahren einen Spitzenplatz in der Tätigkeit der Aufsichtsbehörden ein. Offensichtlich haben Unternehmen weiterhin Probleme, die Videoüberwachung datenschutzkonform umzusetzen. Wir nennen Beispiele und geben Tipps zur Optimierung. Dazu gehört eine neue Leitlinie des Europäischen Datenschutzausschusses.
Weiterlesen: https://www.security-insider.de/videoueberwachung-bei-beschaeftigten-a-916967/?cmp=nl-36&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501

(f) *Personalanalyse – wie weit darf der Arbeitgeber gehen? {IT-Business}*
Bei der Personalanalyse reicht die Spannbreite der berührten Rechtsgebiete vom Datenschutzrecht, über das Arbeitsrecht bis zum Allgemeinen Gleichbehandlungsgesetz. Es kann also eine Menge falsch gemacht werden. Die Forscher der Organisation Algorithmwatch haben sich in zweijähriger Arbeit angesehen, wie solche Softwareanalysen vom Beschäftigen zu bewerten sind. Das Fazit: Viele Unternehmen handeln diesbezüglich womöglich rechtswidrig.
Weiterlesen: https://www.it-business.de/personalanalyse-wie-weit-darf-der-arbeitgeber-gehen-a-909766/?cmp=nl-356&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501

(g) *E-Privacy-Verordnung: Es tut sich etwas an der Cookie-Front {IT-Business}*
Ein neuer Vorschlag für die E-Privacy-Verordnung (ePVO) rüttelt an der notwendigen Einwilligung für Cookies. Doch während die Speicherung von Cookies leichter werden könnte, wollen Browser-Anbieter in Zukunft Drittanbieter-Cookies nicht mehr unterstützen. Doch eigentlich geht es nicht um Cookies oder keine Cookies, es geht um klare Vorgaben und die Information der Betroffenen.

Weiterlesen: https://www.it-business.de/es-tut-sich-etwas-an-der-cookie-front-a-909625/?cmp=nl-43&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501

(h) *Löschkonzepte nach der DSGVO {IT-Business}*
Sobald die ursprüngliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten wegfällt, stellt sich die Frage, ob die Daten gelöscht oder weiter aufbewahrt werden müssen bzw. dürfen. Die gesetzlichen Regelungen erlauben bzw. verlangen je nach Fall unterschiedliches Vorgehen. Verantwortliche müssen deshalb ein Löschkonzept erstellen, das all diese Aspekte berücksichtigt.
Weiterlesen: https://www.it-business.de/loeschkonzepte-nach-der-dsgvo-a-908926/?cmp=nl-356&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501

(i) *Geschäftliche E-Mails: Signatur, Impressum und DSGVO-Pflichtangaben {eRecht24}*
Müssen E-Mails eine Signatur enthalten? Gehört ein Impressum zwingend in geschäftliche E-Mails? Schreibt die DSGVO bestimmte Pflichtangaben in E-Mails vor? Drohen hier teure Bußgelder oder Abmahnungen, wenn diese Vorgaben nicht eingehalten werden? Wir erklären, was Sie zum Thema E-Mailsignatur und DSGVO wissen müssen.
Weiterlesen: https://www.e-recht24.de/artikel/datenschutz/11342-geschaeftliche-e-mails-signatur-impressum-und-dsgvo-pflichtangaben.html

(j) *E-Mails an Warenkorb-Abbrecher: Sind sie rechtlich zulässig? {eRecht24}*
Viele Kunden legen Produkte in den Warenkorb eines Onlineshops, brechen den Kaufvorgang dann aber ab. Clevere Unternehmer versuchen, die potentiellen Kunden durch Erinnerungs-E-Mails und Rabattangebote doch noch zum Kauf zu animieren. Doch sind solche E-Mails überhaupt zulässig?
Weiterlesen: https://www.e-recht24.de/artikel/ecommerce/11015-warenkorbabbrecher-erinnerungsmail-erlaubt-oder-nicht.html

(k) *Bildrechte: So nutzen Sie Bilder rechtssicher auf Webseiten und Blogs {eRecht24}*
Was müssen Sie als Betreiber einer Webseite oder eines Blogs bei der Verwendung von Bildern im Internet beachten? Wo lauern rechtliche Fallstricke und Abmahnungen bei der Nutzung von Bildern? Und viel wichtiger: Wie können Sie diese Abmahnfallen umgehen? Unser Ratgeber zeigt Ihnen die größten Stolperfallen zum Thema Bildrechte im Internet bei Blogs und Webseiten.
Weiterlesen: https://www.e-recht24.de/artikel/blog-foren-web20/7361-so-nutzen-sie-bilder-rechtssicher-in-ihrem-blog.html

(l) *Ulrich Kleber – BfDI: Weitergabe Telekom-Standortdaten datenschutzrechtlich vertretbar*
Die Weitergabe von Standortdaten durch die Deutsche Telekom an das Robert-Koch-Institut @rki_de ist in der gewählten Form datenschutzrechtlich vertretbar. Vor allem unter den aktuellen Umständen spricht nichts gegen die Weitergabe dieser Daten zum Zweck des Gesundheitsschutzes.
Twitter:https://twitter.com/UlrichKelber/status/1240239195236466688

(2) Zu Datensicherheit („TOM“)

(a) *Tipps für sicheres mobiles Arbeiten. Arbeiten von zu Hause oder unterwegs {BSI}.*
TOP 5 der IT-Sicherheit: 1.)„Klar geregelt“ 2.)„Hier gibt es nicht zu sehen“ 3.)“Eindeutig Verifiziert“ 4.)“Vorsicht Phishing“ 5.)VPN
Weiterlesen:https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_mobiles_Arbeiten_180320.html
& PDF BSI: Home-Office? – Aber sicher! (PDF, 240KB, Datei ist barrierefrei/barrierearm)

(b) *Coronavirus: Homeoffice: Technik, Sicherheit, Fallstricke {IT-Business}*
Arbeitnehmer- und Familienfreundlichkeit: Unter diesen Aspekten stand seit Jahren die Arbeit von zuhause. Die Sorge vor einer Ausbreitung des Coronavirus veranlasst viele Arbeitgeber, ihre Angestellten im Homeoffice arbeiten zu lassen.
Weiterlesen: https://www.it-business.de/homeoffice-technik-sicherheit-fallstricke-a-912926/?cmp=nl-356&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501

(c) *Cloud-Apps benötigen mehr als nur Passwortschutz {Cloud-Computing-Insider}*
Viele Cloud-Anwendungen authentifizieren Benutzer ausschließlich mit Passwörtern. Dies ist eine alarmierende Tatsache unter Berücksichtigung der in diesen Systemen gespeicherten sensiblen Daten, die von personenbezogenen Daten (PII) über Zahlungsdaten bis hin zu Betriebsgeheimnissen reichen. Erfahren Sie hier, wie Sie Ihre sensiblen Daten durch Multifaktor-Authentifizierung auch in der Cloud schützen können.
Weiterlesen: https://www.cloudcomputing-insider.de/cloud-apps-benoetigen-mehr-als-nur-passwortschutz-a-900852/

(d) *Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.1 {BSI}*
Dieses Dokument dient als Notfalldokument für IT-Sicherheitsbeauftrage, CISOs und Systemadministratoren von KMU und kleineren Behörden für den Fall eines schweren IT-Sicherheitsvorfalls. Dies kann etwa die Infektion von einer Reihe an Systemen mit einer fortschrittlichen Schadsoftware wie Emotet oder Trickbot oder eine bereits durchgeführte Verschlüsselung mit Ransomware sein. Im Schwerpunkt geht dieses Papier auf die Kombination fortschrittlicher Schadsoftware und Ransomware ein, welche ein gesamtes Netz übernehmen und verschlüsseln kann.
PDF: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf?__blob=publicationFile&v=3

(e) *Zielscheibe: „Mensch“ So schützen sich Unternehmen {Security-Insider}*
Unternehmen sind aufgrund ihrer wertvollen Daten schon lange profitable Ziele für Cyber-kriminelle. Ein Großteil plant deswegen, ihr Budget für Cyber-Sicherheit im nächsten Jahr aufzustocken. Doch geraten auch die eigenen Mitarbeiter in den Fokus der Kriminellen. Durch Social Engineering wird der Mitarbeiter zu einem Sicherheitsrisiko, das man nicht unterschätzen sollte.
Weiterlesen: https://www.security-insider.de/so-schuetzen-sich-firmen-vor-social-engineering-a-912954/?cmp=nl-36&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501

(f) *Gesetzeslage und Anforderungen an IT-Sicherheit in der Zukunft {IT-Business}*
Das Thema IT-Sicherheit betrifft im Rahmen der Digitalen Transformation immer mehr Branchen und somit Menschen. Je breiter ein Marktumfeld wird, desto wichtiger wird eine umfassende Standardisierung, um sicherzustellen, dass Sicherheitsaspekten stets genügend Raum gegeben wird.
Weiterlesen: https://www.it-business.de/gesetzeslage-und-anforderungen-an-it-sicherheit-in-der-zukunft-a-912751/?cmp=nl-356&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501

(g) *Neue Sicherheitsrisiken durch Sprachassistenten {IT-Business}*
Wer seinen Arbeitsplatz oder sein Smartphone verlässt, tut gut daran, das Gerät zu sperren, sonst können unautorisierte Personen unter fremden Namen Botschaften verschicken, Waren bestellen oder wichtige Dateien löschen. Was aber, wenn dazu einfach ein Stimmbefehl ausreicht?
Weiterlesen: https://www.it-business.de/neue-sicherheitsrisiken-durch-sprachassistenten-a-910778/?cmp=nl-43&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501

(h) *Angreifer können WPA2 hacken {Security-Insider}*
Kr00k gefährdet Millionen WLAN-Geräte. Durch die Sicherheitslücke CVE-2019-15126, auch Kr00k genannt, können Angreifer WLAN-Chips der Hersteller Broadcom und Cypress

belauschen, auch dann, wenn der Verkehr mit WPA2 gesichert ist. Betroffen sind Millionen Geräte von Amazon, Apple, Samsung, Google und vielen anderen Herstellern.
Weiterlesen: https://www.security-insider.de/kr00k-gefaehrdet-millionen-wlan-geraete-a-912820/?cmp=nl-36&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501

(3) Zu übergreifenden Themen

(a) Home Office: Was Unternehmer und Mitarbeiter zu Datenschutz und Arbeitsrecht beachten müssen {eRecht24}

Deutschland ist im Ausnahmezustand: Das Virus hat auch uns erreicht und ist laut nun offiziell eine Pandemie. Um eine schnelle Verbreitung des Virus zu verhindern schicken immer mehr Arbeitgeber ihre Mitarbeiter ins Homeoffice. Aber geht das arbeitsrechtlich überhaupt so einfach? Was muss aus Gründen der IT-Sicherheit beachtet werden? Und haben Sie an eine DSGVOkonforme Vereinbarung mit Ihren Mitarbeitern gedacht?
Weiterlesen: https://www.e-recht24.de/artikel/arbeitsrecht/11972-corona-home-office-datenschutz-arbeitsrecht.html

(b) Gut 40 Prozent deutscher Unternehmen erleben Cyberangriffe {IT-Business}

In den vergangenen zwölf Monaten haben laut einer Studie vom Kriminologische Forschungsinstitut Niedersachsen 41 Prozent der deutschen Unternehmen mit mehr als zehn Beschäftigten auf mindestens einen Cyberangriff reagieren müssen. In dieser Berechnung seien automatisiert abgewehrte Angriffe wie zum Beispiel von einer Firewall gestoppte Spam-E-Mails nicht enthalten.
Weiterlesen: https://www.it-business.de/gut-40-prozent-deutscher-unternehmen-erleben-cyberangriffe-a-913897/?cmp=nl-43&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501

(c) Psychisches Hacking der „Schwachstelle Mensch“ {Security-Insider}

Der Kampf gegen Social Engineering wird häufig auf das Aussortieren der lästigen Phishing-Mails reduziert. Dabei nutzen Angreifer noch ganz andere Taktiken für ihr Ziel: den Menschen. Mit Kniffen, tief aus der psychologischen Trickkiste, triggern sie diverse Verhaltensmuster. Das Vorgehen ähnelt stark dem der Figur des Hauptmanns von Köpenick.
Weiterlesen: https://www.security-insider.de/psychisches-hacking-der-schwachstelle-mensch-a-912554/?cmp=nl-36&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501

(d) Coronavirus macht Homeoffice zum Hacker-Ziel {Security-Insider}

Das Coronavirus hat Europa und viele andere Länder der Welt fest im Griff. Um die Ansteckungsfälle soweit wie möglich zu reduzieren bleiben Restaurants und Geschäfte geschlossen und Homeoffice wird für viele Angestellte immer mehr zum Alltag. Dadurch steigt allerdings die Gefahr, dass Mitarbeiter eines Unternehmens Opfer von Social Engineering- oder Phishing-Versuchen werden.
Weiterlesen: https://www.security-insider.de/coronavirus-macht-homeoffice-zum-hacker-ziel-a-914882/?cmp=nl-36&uuid=96BDE5EF-F3A6-43FF-90A0900F882EC501