FH Burgenland
UNIVERSITY OF APPLIED SCIENCES
Department Informationstechnologie und Informationsmanagement

Masterarbeit

Auswirkung der EUDSGVO auf die Nutzung von Cloud-Diensten für ein fiktives KMU im Bereich Webdesign, bzw. -programmierung.

zur Erlangung des akademischen Grades
Master of Science in Engineering

Masterstudiengang Cloud Computing Engineering

Eingereicht von: Mag. Christian Gossmann, BSc
Personenkennzeichen: 1710781010
Datum: 13. Juni 2019

Betreut von: Leopold Obermeier MBA, MSc

Vorwort

Diese Arbeit entstand aus beruflichem Interesse als Systemadministrator heraus, Auswirkungen der EUDSGV zu betrachten. Da auch Privatpersonen davon betroffen sind, wenn z.B. nur Affilliate-Programmcode auf einer Webseite abgerufen wird und personenbezogene Daten an das jeweilige Unternehmen überträgt, muss dies EUDSGVO-konform geschehen, um nicht mit Strafen konfrontiert zu werden. Thematisch knüpft die Arbeit hinsichtlich des Datenschutzes an meine damalige Diplomarbeit: „Implementierungsstrategien und Auswirkungen auf Datenschutz- und Urheberrechte vor dem Hintergrund der Internetkommerzialisierung“ von 2006 an. Heute hat sich bestätigt, wie wahr die damalige Schlussfolgerung war – leider muss man fast schon gestehen:

> „Vieles ist auch beim Datenschutz strittig, dabei jedoch v.a. bezüglich der unterschiedlichen Ansichten in den USA und Deutschland, sowie dem Interesse der Nutzer, hier nicht überwacht zu werden. Schwachpunkte bestehen hier bei allen Formen von DRMS hinsichtlich der Wahrung des Datenschutzes. Da Content vornehmlich aus den USA kommt und dort Datenschutz eher ein Fremdwort ist, liegen hier lediglich freiwillige Zusagen in Form von Gütesiegelprogrammen vor. Forcierte Safe Harbor Príncipes gewähren hier wenigstens dem Papier nach die Einhaltung europäischen Datenschutzniveaus auch bei Datenverarbeitern in den USA. Problematisch ist aber, dass man hier kaum Kontrollmöglichkeiten hat.“ (Gossmann, 2006, S.144)

Damals wurden die USA und Deutschland betrachtet und das einleitende Zitat von Rechtsprofessor Lawrence Lessig „Die technische Bedrohung ist maximal, der vom Gesetz gebotene Schutz dagegen nur noch minimal.“ (nach Gossmann, 2006, S.5) bezog sich auf digitale Güter und deren Vervielfältigungsmöglichkeiten. Daten zählen allerdings auch zu „kopierbaren Gütern“. Somit war bekanntlich bis zur Verabschiedung der EUDSGV 2016 ebenfalls vieles strittig, das bis 2018 noch national geregelt wurde und nunmehr vereinheitlicht ist. Personen wollen ihre Daten geschützt wissen, Datenschutz in den USA heißt allerdings noch immer Schutz der Daten für Unternehmen und nicht Datenschutz im Sinne von Personen. Safe Harbor entpuppte sich tatsächlich als „Schutz dem Papiere nach“ - bekanntlich wurde es durch Maximilian Schrems zu Fall gebracht (Katulic, Vojkovic, 2016, S.1447) und Kontrollmöglichkeiten bestehen nach wie vor nicht, v.a. was aufkommende Cloud-Lösungen anbelangt, die, wenn nicht aufgepasst wird, u.U. in

Rechenzentren von Microsoft, Google oder Amazon und somit bei US-Unternehmen landen – auch hier soll die EUSDGVO entgegenwirken. Die Arbeit versteht sich somit als logische Fortsetzung von damals, lässt jedoch Digital Rights Management und Urheberrechte weitgehend außer Acht, da viele Änderungen weg vom Datenträger hin zum Streaming erfolgt sind. Stattdessen liegt der Fokus auf Auswirkungen für ein fiktives Webdesign-KMU, das darauf achten muss, wo seine Daten gespeichert und Produkte gehostet werden, um nicht bestraft zu werden. Bedanken möchte ich mich für die Anregungen während des Verfassens dieser Arbeit bei meinem Betreuer Leopold Obermeier MBA, MSc und Dr. Markus Tauber für die Tipps in den zugehörigen Masterarbeit begleitenden Seminaren.

Christian Gossmann
Eisenstadt, 11. Juni 2019
www.Gossmann.at

Inhaltsverzeichnis

Kurzfassung

Diese Arbeit behandelt Auswirkungen der seit 25.5.2018 in der EU geltenden Datenschutzgrundverordnung auf ein fiktives Webdesign-KMU. Ziel ist, Datenschutz griffiger zu machen, indem Auskunfts-, Richtigstellungs- und Löschrechte durchsetzbar werden. Diese gab es zwar auch schon früher in nationalen Datenschutzgesetzen, doch sieht die EUDSGVO Vereinheitlichung und hohe Strafen für Verstöße bis vier Prozent Jahresumsatz oder 20 Mio. Euro vor. Damit wird v.a. auf Großkonzerne wie Facebook und Google gezielt. Das Problem ist allerdings, auch kleine und mittlere Unternehmen in deren Existenz zu bedrohen, da Daten – eine Kundendatenbank reicht - de facto überall verarbeitet werden. Besonders als Webdesign-KMU ist man durch technische Funktionsprinzipien des Internets besonders davon betroffen, wobei nur IP-Adressen, Cookies und Log-Files zu nennen wären. Diese Prinzipien waren vor Inkrafttreten der EUDSGVO selbstverständlich, können aber nun bei falscher Handhabung geahndet werden. Die Strafen sind dabei für jeden einzelnen Verstoß vorgesehen, was die existenzbedrohende Gefahr verdeutlicht. Behandelt werden typische Webdesign-Bereiche, wie Development, Grafikdesign, Datenbanken und Hosting, wo es um die Sammlung und Kontrolle der Übermittlung von Daten geht, was auch Drittstaaten anbelangt. Dies ist v.a. bei redundanten Rechenzentren der Fall, die als Auftragsverarbeiter für die Webdesign-KMUs, bzw. deren Kunden fungieren. Webdesign-KMUs selbst treten nämlich selten auch als Hoster auf. Dass Probleme durch Pflichten zum Ändern, Richtigstellen und Löschen, was - wie gezeigt wird, vielfach gar nicht möglich ist, auftreten, wird dabei deutlich. Dies betrifft sowohl Technik wie Backups. Die Auswirkungen werden dabei mit Metriken in Form wichtiger Kennzahlen aus der Betriebswirtschaftslehre einmal unter Berücksichtigung der EUDSGVO als auch ohne gemessen. Methodisch wurde eine Literaturrecherche durchgeführt und um realistische Zahlen zu erhalten, eine Inhaltsanalyse. Erwartetes Ergebnis waren deutlich negative Auswirkungen. Es wurde allerdings deutlich, dass dem nicht so ist und die EUDSGVO sich sogar positiv auswirkt. Negative Auswirkungen waren lediglich von kurzer Dauer und sogar durch das operative Tagesgeschäft meist mit bestehendem Personal abzufedern.

Abstract

This study examines the impact of the GDPR of the EU, that is law since 28.5.2018 on a fictional web design small and medium-sized business. The goal is to make data protection more effective by allowing people to enforce information, correction and deletion rights. Although these were already national law in each membership country, the EUDSGVO provides unification and high penalties for violations that are up to four percent annual turnover or 20 million €. This aims at large companies such as Facebook and Google. However, the problem is, that even small and medium-sized businesses are threatened in their existence, as data processing – e.g. a simply customer databases - is used everywhere. Especially a web design small and medium-sized business is affected by technical operating principles of the Internet, only to be mentioned the IP address, cookies and log files. Even these principles were in use before the EUDSGVO was law, wrong handling can lead to penalties now. The penalties are provided for each individual infringement, which demonstrates the existence-threatening danger. This paper covers typical areas of web design, such as development, graphic design, data bases and hosting. That means collecting and controlling the transfer of data, which might include non EU-countries. Especially redundant data centers are affected by this regulation, which act as data processor for the web design small and medium-sized business or their customers, as they seldom operate a data center for hosting themselves. That problems arise in obligations to modify, correct and delete data, which - as shown, will often not even be possible - becomes clear. This includes technology as well as backups. Effects are measured with important metrics of operational economics, once with and without the impact of the GDPR. Methods used are a literature research and in order to get realistic data for the fictional web design small and medium-sized business a content analysis has been done. The expected result are negative effects on the metrics due to the GDPR. However, during the work on this paper, it got more and more clear, that this is not the case and that the GDPR in opposite has positive effects. Negative effects were only of short duration and can be handled mostly by already existing staff.

Keywords: impact, GDPR ,cloud, hosting, webpage, website, www, cookies

1 Einleitung

1.1 Problemstellung

Unternehmen zu leiten erfordert heute, sich mit umfangreichen Aufgaben auseinanderzusetzen. Gemeint ist dabei der operative Betrieb mittels IT, ohne die heutzutage de facto nichts mehr läuft. Zu nennen wäre nur die Bestellung von Verkaufswaren oder die Personal-, Kunden- und Auftragsverwaltung. Verschärft wurde diese Problematik neben Regelungen zur Registrierkassen-, Rechnungslegungs-, bzw. Buchhaltungs- und Bilanzierungspflichten der vergangenen Jahre durch die kürzlich in Kraft getretene europäische Datenschutzgrundverordnung (EUDSGVO). Während sich Einzelhändler mit geringen Umsätzen ohne doppelte Buchführungspflicht noch mit vergleichsweise günstiger Standard-Office-Software behelfen können, gilt dies für größere Unternehmen und KMUs v.a. bei der EUDSGVO nicht mehr. Hier müssen Verzeichnisse geführt werden, welche Datenverarbeitungen im Unternehmen erfolgen. Eine Excel-Tabelle reicht zu diesem Zweck kaum mehr, weshalb deutlich wird in teure Spezialsoftware investieren zu müssen. Die EUDSGVO trifft dabei alle, die auf irgendeine Art personenbezogene Daten verarbeiten. Ein Lieferanten- oder Kundenverzeichnis reicht dafür bereits aus. Damit sind Einzelhändler, KMUs und Großkonzerne gleichermaßen betroffen. Während letztere jedoch häufig über hohe Reserven an liquiden Mittel verfügen, um die EUSDGVO umzusetzen, dürfte dies bei KMUs nicht immer der Fall sein. Abstriche bei der Umsetzung der EUDSGVO zu machen, ist jedoch höchst riskant, da die angedrohten Strafen existenzbedrohend sind. Bei gravierenden Verstößen drohen Strafen bis zu 20 Mio. Euro oder 4% des Jahresumsatzes, je nachdem, welche Summe höher ausfällt (Art. 83 Abs. 5. EUDSGVO).

Neben der Einführung von mit dem Datenschutz beauftragten Personen (Art. 37 EUDSGVO), stellt sich auch die Frage nach der richtigen IT-Ausstattung. Bisher war es gängige Praxis, Server und Client-Hardware sowie entsprechende Software-Lizenzen zu beschaffen, wobei durchaus auch Spezialprodukte zum Einsatz kommen konnten - je nach Unternehmenstätigkeit. Dafür wurden entsprechende Schulungsmaßnahmen gesetzt sowohl für Personal wie für die

Systemadministratoren. Ferner musste die Hardware auch noch verstaut werden, was entsprechende Räumlichkeiten voraussetzte, konkret geschah dies in gesicherten Serverräumen mit Brandmeldern, Löschsystemen, unterbrechungsfreier Stromversorgung, Monitoring-Tools, etc... Als ob dies noch nicht genug wäre, erforderte der Betrieb derartiger IT neben qualifizierten Systemadministratoren auch regelmäßige Wartungs- und Adaptierungskosten für neue Software, d.h. Updates, wenn der Hersteller der Systeme nicht mehr bereit war, ältere Versionen zu unterstützen, was natürlich auch mit entsprechender Ressourcenbindung beim Hersteller zu tun hatte. Damit einhergehend war der Zwang für dessen Kunden verbunden, meist auch auf neue, leistungsfähigere Hardware umzurüsten, was mit erheblichen Kosten verbunden war. Diesen Schritt jedoch zu unterlassen wäre gleichbedeutend mit Fahrlässigkeit, da in älteren Systemen faktisch immer Sicherheitslücken zu finden sind, die bei Ausnutzung zu Datenmanipulation und Datenschutzverletzungen führen können.

Zusammengefasst musste man also jederzeit damit rechnen, alle paar Jahre die gesamte IT-Landschaft im Unternehmen auszuwechseln, was neben den Anschaffungs- und Betriebs- auch neuerlich entsprechende Folgekosten für Umschulungen oder Migration älterer Daten verursachte. Somit ist klassische IT ein entsprechend hoher Kostentreiber im Unternehmensumfeld gewesen. Strategien günstiger ans Ziel zu kommen fand man in den letzten Jahren in Cloud-Diensten, die erhebliches Einsparungspotential im Unternehmensumfeld boten. Genau darin liegt das Problem, denn aktuell läuft man Gefahr, durch den Zwang in Hinblick auf die existenzbedrohenden Strafen konform der EUDSGVO sein zu müssen, diesen Vorteil wieder ins genaue Gegenteil zu verkehren. Der Grund dafür liegt in der Speicherung von Unternehmensdaten „außerhalb“ des eigenen Umfeldes, eben in der Cloud. Haben Unternehmen aber nicht mehr die volle Kontrolle über Daten on-premises, so greifen diverse Verpflichtungen der EUDSGVO, sich davon zu überzeugen, ob ein entsprechendes Schutzniveau für die Daten besteht und entsprechende Auftragsverarbeiterverträge mit Cloud-Anbietern abgeschlossen wurden (Art. 28 EUDSGVO). Man haftet nämlich als

Unternehmen für Datenschutzverstöße des Auftragsverarbeiters. Genau diese Furcht veranlasst Unternehmen ihre derzeitige Cloud-Strategien vor den Hintergrund der EUDSGVO zu überdenken. Die These in dieser Arbeit lautet daher: die EUDSGVO bremst die Auslagerung von Services durch Unternehmen in die Cloud. Untersucht werden soll, ob dies tatsächlich zutreffend ist und eine Verteuerung der angebotenen Produkte und Services dieser Unternehmen bedeutet, wenn CAPEX- wie auch OPEX-Ausgaben infolge dessen steigen. Werden nämlich neue Betriebsumgebungen mit Datenschutz- und Spezialsoftware erforderlich, bedingt dies auch neue Server und entsprechend geschultes Personal zu dessen Bedienung und Support. Wie Abbildung 1 des Zentrums für Europäische Wirtschaftsforschung zeigt, sind diese Bedenken auch nicht unbegründet, da mehr als, bzw. fast die Hälfte der Unternehmen erhöhte Kosten, mehr Arbeitsaufwand und verkomplizierte Geschäftsprozesse fürchten, was letztlich einen Wettbewerbsnachteil gegenüber Unternehmen in Drittstaaten darstellt. Etwa 20% befürchten sogar ein Bremsen von Innovationen.

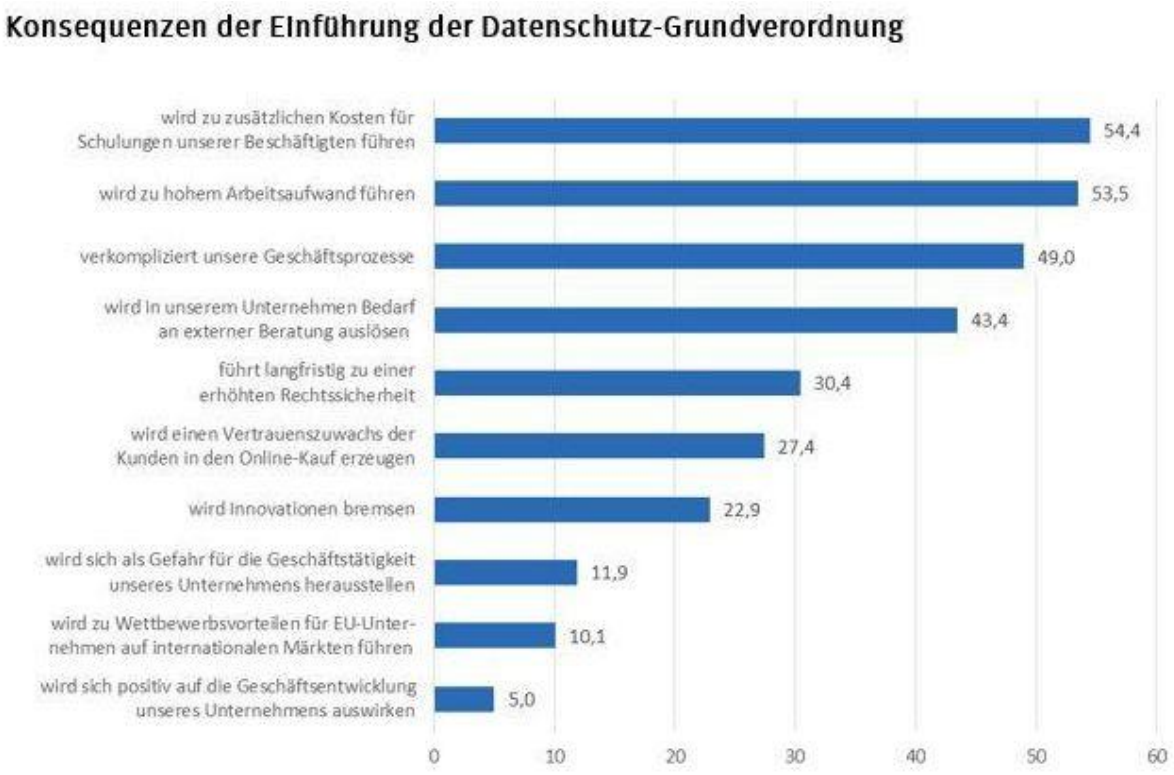


Abb. 1: Konsequenzen der Einführung der EUDSGVO. (Ohnemus, 2018)

Konkret sollen in der Arbeit am Beispiel eines fiktiven KMUs zur Erbringung von Dienstleistungen im Bereich des Webdesigns- und –programmierung die Auswirkungen der EUDSGVO auf dieses überprüft werden, inwieweit obige Befürchtungen zutreffend sind, welche Änderungen, aber auch Vorteile sich letztlich dadurch ergeben und ob diesbezüglich tatsächlich eine Verteuerung der Leistungen durch die EUDSGVO eintritt. Der Fokus liegt dabei bei den zur Methodik angeführten Use Cases: Datenbank, Grafik-Software, Hosting und Development. Diese werden dabei sowohl mit als auch ohne zugrunde gelegter EUDSGVO betrachtet. Die Metriken dafür stellen anerkannte, betriebswirtschaftliche Kennzahlen dar, die ebenfalls bei der Methodik noch im Detail genannt werden. Was bei den Metriken den betrachteten Grad des Datenschutzes anbelangt, so liegt der Fokus auf der Umsetzung gesetzlichen Vorgaben durch die EUDSGVO. Konkret geht es also um zwingend notwendigen Reaktionen auf geänderte Rahmenbedingungen in Form von zu tätigenden Umrüstungs-, bzw. Erweiterungsmaßnahmen von Weblösungen. Der Problemnachweis es hier tatsächlich mit geänderten Rahmenbedingungen zu tun zu haben, ist für jeden ersichtlich, der im World Wide Web Seiten aufruft. Man wird plötzlich mit unerwarteten Cookie-Hinweisen konfrontiert, teilweise sind Webseiten in den USA wie die L.A.-Times für europäische Clients durch Geoblocking nicht mehr erreichbar, eingebundener Content von sozialen Netzwerken muss erst bestätigt werden und Unternehmen, die aus Kostengründen moderne Messenger wie Whatsapp einsetzten, mussten diese deinstallieren. Dies deswegen, da hier die Gefahr besteht, unbewusst Daten wie eben der Telefonbücher des Smartphones an die Betreiber zu übertragen. Derartiges stellt immer dann einen EUDSGVO-Verstoß dar, wenn dies ohne Einwilligung geschieht - und eine solche von dutzenden oder hunderten Kontakten im Vorfeld einzuholen ist eben nicht praktikabel. Genauswenig lässt sich kaum das Einverständnis sämtlicher Webseitenbesucher stillschweigend voraussetzen, wenn Drittcontent wie eben solcher aus sozialen Netzwerken angezeigt werden soll.

1.2 Zielsetzung und wissenschaftliche Fragestellung

Konkret wird folgender Forschungsfrage nachgegangen: wie kann man Cloud-Systeme nach Inkrafttreten der EUDSGVO nutzen, um einerseits konform zu dieser zu bleiben, andererseits die Kosten für die IT auch weiterhin zu senken? Wählte man bisher die erstbeste Cloud-Lösung eines Anbieters und waren Daten dabei in Rechenzentren außerhalb der EU gehostet, das Unternehmen jedoch auf europäischem Boden tätig, so unterliegt es seit 25. Mai 2018 vollumfänglich den Datenschutz-Verpflichtungen und existenzbedrohendem Strafrahmen der EUDSGVO. Verschärft wird dieser Umstand dadurch, die großen Big Player wie Google Cloud, Amazon Webservices und Microsoft Azure als US-Unternehmen außerhalb der EU vorzufinden, wo bekanntlich US-Präsident Donald Trumps kürzlich verordneter Cloud Act den Zugriff auf Daten auf außerhalb den USA liegenden Rechenzentren ermöglicht, wenn zumindest ein US-Unternehmen daran beteiligt ist. Problematisch für Unternehmen ist allerdings, sog. Redundanz bezogen auf störungsfreien 24/7-Betrieb nur dann gewährleisten zu können, wenn Failovers möglich sind. Fallen ganze Regionen durch Naturkatastrophen, Terror oder menschliches Versagen z.B.: in der Stromversorgung aus, so muss weltweit auf verteilte Rechenzentren zurückgegriffen werden. Damit wäre man als Unternehmen nun dahingehend eingeschränkt, nur Rechenzentren zu wählen, die in der EU von nicht US-Unternehmen betrieben wären oder auf weltweit verteilte Sicherheit im Betrieb zu verzichten.

Dabei stellt sich die erste Unterfrage, welche Daten überhaupt bei Cloud-Anbietern gespeichert und verarbeitet werden dürfen, also z.B. keine sensiblen medizinischen Daten. Zudem geht es um Daten, die zwar nicht unter die EUDSGVO fallen, Unternehmen allerdings dennoch als geschäftskritisch erachten, d.h. konkret solche, die im Verlustfall ebenfalls die Existenz gefährden. Zu denken wäre z.B. an Betriebs- und Geschäftsgeheimnisse, bzw. verfahrenstechnische Daten in der Industrie oder militärisches Material. Hier gilt es somit nach der Art der Daten zu klassifizieren, die man – allen Vorteilen der Cloud zum Trotz –aus Angst vor erleichterter Spionage, sowohl industrieller wie

militärischer Natur besser on-premises behält. Gibt es nämlich zentrale Anlaufstellen, wie eben Rechenzentren von Cloud-Anbietern und schaffen es Behörden, die dann zumeist legal bei der Strafrechtspflege tätig werden oder Konkurrenzunternehmen auf illegale Weise wie auch Kriminelle deren Sicherheitsbarrieren zu überwinden, fallen ihnen faktisch sämtliche Daten aller Kunden in die Hände. Deswegen stellen sich geradezu für ein Unternehmen im Bereich des Webdesigns- und –programmierung genau solche Herausforderungen, die Requirements ihrer Auftraggeber genauestens abzuschätzen und EUDSGVO-fest zu implementieren.

Die zweite Unterfrage beschäftigt sich mit eben jenen möglichen Vorteilen der EUDSGVO. Immerhin erblicken fast 30% in Abbildung 1 einen Vertrauenszuwachs, 10% trotz allem einen Wettbewerbsvorteil und 5% sehen immerhin eine positive Geschäftsentwicklung. D.h. konkret, hier mit zusätzlichen Auftragsvolumina rechnen zu können, die man dann gerade deswegen erhält, weil man die Daten der Auftraggeber besser zu schützen zu vermag als dies vor Inkrafttreten der EUDESGVO der Fall gewesen wäre. Hierdurch können sich entsprechende Synergieeffekte ergeben und es lässt sich ein guter Ruf des Unternehmens aufbauen.

Related Work:

An Related Work existieren zu obigen Fragen bis dato zwar reichlich Abhandlungen über die EUSDSGVO und deren Auswirkungen für Unternehmen. Die Palette reicht dabei vom EUDSGVO-konformen Löschen von Daten (Berning, Wilhelm & Meyer, Kyrill & Keppeler, Lutz., 2018), deren technische und rechtliche Probleme (Keppeler, Lutz & Berning, Wilhelm, 2017) über allgemeine Diskussionen bezüglich der Auswirkungen schon zum Zeitpunkt des Erlasses der Verordnung und damit fünf Jahre vor deren Inkraftreten (Eckhardt, Jens & Kramer, Rudi, 2013) sowie Handlungsempfehlungen für die Politik (Ute & Ruhmann, Ingo & Schuler, Karin & Weichert, Thilo, 2016) bis hin zu Rechten betroffener Personen (Voigt, von dem Bussche, 2018). Den Auswirkungen auch vor dem Hintergrund allfälliger

Vorteile, konkret für ein KMU im Bereich Webdesign- und -programmierung hinsichtlich der bei der Forschungsmethodik genannten vier Teilaspekte Datenbanken, Grafik-Software, Hosting und dem eigentlichen Development hat sich jedoch noch niemand in dieser Form angenommen. Auch hier existieren bisher nur allgemeine Richtlinien, wie z.B. seitens der Wirtschaftskammer Österreich Empfehlungen, wie denn Webseiten konkret hinsichtlich Cookies, Log-Dateien und Auswertungen von Formularen nach Inkrafttreten der EUDSGVO gestaltet werden sollten. (WKO, 2019).

Schütz und Gneisz bringen diesen Umstand treffend auf den Punkt:

„Bei einer anfänglichen Betrachtung der umfangreichen Verpflichtungen, die auf ein Unternehmen zur Einhaltung der DSGVO-Vorgaben zukommen, wird möglicherweise die Erwartung des Eintretens „des Scheiterns" größer sein als jene, damit auch eine Reihe wirtschaftlich wirklich interessanter Vorteile für sein Unternehmen zu erschließen. Das ist aber damit ganz konkret möglich! Diese positiven Effekte von DSGVO-Projekten müssen in die kaufmännische Gesamtbetrachtung integriert werden. Sie sind vielfältig und natürlich von Fall zu Fall verschieden." (Schütz, Gneisz, 2017, S.4)

Detaillierter wird darauf im Kapitel zur Related Work in der Arbeit noch eingegangen, v.a. hinsichtlich der betroffenen Cloud-Services wie PaaS, SaaS und IaaS.

1.3 Ziele sowie Nutzen der Arbeit

Als Ergebnis wird erwartet, mit entweder mehr positiven oder negativen Auswirkungen rechnen zu müssen. Ziel ist es daher, diejenigen Strategien aufzuzeigen, wie aus der EUDSGVO ein optimaler Nutzen gezogen wird, sowohl Datenschutz einerseits und Kostenersparnis durch Cloud-Services andererseits zu gewährleisten. Ziel ist ferner, dem KMU die Furcht vor allfälligem künftigen Nicht-Nutzen von Cloud-Services zu nehmen. Zur Erinnerung sei nämlich darauf hingewiesen, dass die EUDSGVO unabhängig von der Nutzung von Cloud-Services gilt. Verstößt ein Unternehmen dagegen, spielt es somit keine Rolle, ob es um Services on-premises oder in der Cloud geht. Es soll daher gezeigt werden, die Cloud als Chance zu sehen, diese jedoch vor dem Hintergrund der EUDSGVO richtig im Sinne auslagerungsfähiger Daten und Services zu nutzen.

Insofern besteht die praktische Relevanz dieser Arbeit im Aufzeigen von Strategien zur Vermeidung der vorgesehenen existenzbedrohenden Strafen, was in den jeweiligen Kapiteln zu den einzelnen Teilbereichen, die in der Methodik genannt werden, geschieht.

1.4 Nicht-Ziele

Es ist nicht Ziel, Interessen des Data Mining durch Auftraggeber zu behandeln. Auch wird kein Vergleich zwischen konkreten Anbietern von Cloud-Lösungen durchgeführt, wer wie gut den Datenschutz umsetzt. Diesen Vergleich müssen letztlich die Unternehmen selbst von Zeit zu Zeit durchführen, denn Ziel ist lediglich die Rahmenbedingungen im Zeitpunkt des Auftrages vor dem Hintergrund der EUDSGVO zu beachten. Ein Längsschnitt-Vergleich kann schon allein deshalb nicht erfolgen, da hier nur der Use Case „KMU mit Webdesign- und -programmierung" betrachtet wird, es allerdings im weiteren Umfeld auf den jeweiligen Geschäftsbereich des Auftrag-Unternehmens ankäme, der sich im Laufe der Zeit natürlich wandeln kann, was hieße, implementierte Lösungen unter Umständen nicht mehr EUDSGVO betreiben zu können. Würde z.B. ein Chemieunternehmen plötzlich auch medizinische Produkte herstellen und diesbezüglich Patientendaten erheben so liegen gänzlich andere Voraussetzungen für die Produktdatenbank vor, denn mit medizinischen Daten ist eben anders zu verfahren. Um dennoch auf entscheidende Probleme eingehen zu können, gilt für das hier behandelte fiktive KMU im Bereich Webdesign- und -programmierung, die entsprechenden Auftraggeber und deren Daten im Auftragszeitpunkt genauestens kennen zu müssen. Erst dann können EUDSGVO-konforme Lösungen angeboten werden. Ferner wird in der Arbeit auch nicht auf urheberrechtliche Problematiken, die bei Datenschutzverletzungen entstehen könnten, eingegangen. Hier bieten sich somit noch reichlich Betätigungsfelder für Forschungsarbeiten im juristischen Umfeld.

1.5 Forschungsmethodik

Es wird eine Literaturrecherche durchgeführt, um im Zuge einer theoriebasierten Exploration vorhandenes Wissen einer Neubewertung zu unterziehen.

Herangezogen werden dabei auch bereits vorhandene grafische Darstellungen ergänzt um eigene Kostentabellen. Um an das dazu erforderliche verwertbare Zahlenmaterial zu gelangen, wird eine Inhaltsanalyse mach Mayring (2015, S.9ff.) durchgeführt. An Quellen kommen dabei facheinschlägige Job-Inserate, verfügbare Preislisten, Geschäfts- und Personalberichte, Nachrichten mit Bezug zur Wirtschaft oder bereits als wissenschaftliche Studien vorliegende Erhebungen in Frage. Fundstellen werden dabei - sofern im Internet vorhanden, abgespeichert, bzw. falls nur in Printform vorliegend, digitalisiert und danach abgespeichert, um auch diese belegen zu können und Nachvollziehbarkeit der Auswertung zu gewährleisten.

Für die Auswertung selbst wird dabei deduktiv vorgegangen, wobei das Quellmaterial nach festgelegten Auswertungskategorien auf entsprechende Fundstellen hin untersucht wird. Die Kategorien stellen dabei nachfolgende aus der Betriebswirtschaftslehre und dem Rechnungswesen stammenden Kennzahlen dar, womit eine eindeutige Zuordnung dann möglich wird, wenn entsprechende Zahlen oder prozentuelle Angaben im Quellmaterial dazu vorliegen oder zumindest Rohdaten genannt werden, die für deren Berechnung erforderlich sind. Sollte eine eindeutige Zuordnung nicht möglich sein, was durch die erwartete Diversität des Materials als Gegeben anzunehmen ist, gilt es anhand von Kodierregeln eine eindeutige Zuordnung zu treffen. Diese Kodierregeln werden im Laufe der Arbeit entwickelt, wobei der erforderliche Kodierbogen während der Gewinnung des Datenmaterials in mehreren Sichtungs-Durchläufen zu adaptieren ist. Dazu wird das Quellmaterial so lange gesichtet, indem entsprechende Verfeinerungen durch die von Mayring vorgesehenen Paraphrasierungen, Zusammenfassungen und Überarbeitungen erfolgen bis die erforderlichen Daten in nicht mehr weiter differenzierbarer Form vorliegen (2015, S.36ff.).

Für die dazu notwendige Vorerhebung dienen dabei erst einmal fünf Fundstellen betreffend jeden Bereich der unten aufgelisteten Variablen, die für ein Unternehmen im Bereich des Webdesigns- und -programmierung typisch sind, nämlich Cloud-Lösungen im Bereich:

- Datenbanken → sowohl zur Personalverwaltung, wie auch operativen Betrieb der Services
- Grafik-Software → zur Erstellung von Webcontent
- Hosting → zur eigentlichen Plattformbereitstellung
- Development → die eigentlichen Programmiertätigkeit und Entwicklung mittels Content-Managment-Systemen

Da eben Zahlenmaterial von primärem Interesse ist, ist es v.a. wichtig nicht blindlings z.B. nach dem Begriff „Umsatz" zu suchen, sondern darauf zu achten, hier eben Umsätze in selben Zeiträumen zu betrachten. Konkret geht es also um das sprichwörtliche Suchen des gemeinsamen Nenners und nicht um den Vergleich von Äpfeln mit Birnen. In die eigentliche Auswertung sollen dann 20 Fundstellen einfließen. Folgende Ankerbeispiele dienen exemplarisch als Anhaltspunkt für die Zuordnung zu den folgenden fünf betrachteten Metriken:

- **Cashflow** → um den Spielrahmen für Investitionen im jeweiligen Bereich zu veranschaulichen
  Ankerbeispiel:
  „Die auf die Entwicklung und Betreuung von Webauftritten spezialisierte Web 2.0 GmbH erzielt mit acht Mitarbeitern einen Umsatz von 890.000 € und einen Jahresüberschuss von 210.000 €. Das Unternehmen verfügt über acht hochwertige Arbeitsplätze. Der bisherige alleinige Gesellschafter und Geschäftsführer (A) möchte sich nun mehr um die strategische Ausrichtung kümmern und bietet einem seiner Mitarbeiter (B) eine 25-prozentige Beteiligung an."
  Quelle: https://t3n.de/magazin/wert-eigenen-web-startups-kennen-unbezahlbar-226103/ [01.01.2019]
- **Verschuldensgrad** → wobei dieser vom Eigen- und Fremdkapital abhängt
  Ankerbeispiel:
  „Die Top100 deutschen Aktiengesellschaften mit dem niedrigsten Verschuldungsgrad" - die konkrete Zahlenauflistung folgt auf der Webseite.
  Quelle: https://www.finanzen100.de/top100/die-deutschen-

aktiengesellschaften-mit-dem-niedrigsten-verschuldungsgrad/ [01.01.2019]

- **Personalkosten in Prozent der Betriebsleistung** → damit die Personalintensität

  Ankerbeispiel:

  „Der Mitarbeiter muss etwa das 2,5-fache der für ihn anfallenden Personalkosten erwirtschaften, damit es sich lohnt, ihn einzustellen." Quelle: https://www.unternehmerlexikon.de/personalkosten-berechnen/ [02.01.2019]
- **Return on Sales** → damit die Gewinnsituation des Unternehmens

  Ankerbeispiel:

  „Wir möchten als Full-Service-Agentur den kleinen und mittleren Betrieben, die keine großen Onlinebudgets von hunderten tausenden Euro haben, helfen ihre digitale Identität zu finden, ihre Dienstleistungen und Produkte anzubieten und ihre Kunden in der digitalen Sphäre wiederzufinden."

  Quelle:

  https://firmen.wko.at/Web/DetailsKontakt.aspx?FirmaID=b36aeb70-6fe6-46c1-b2d4-73179900fee0 [02.01.2019]
- **Return on Investment** → damit die Rentabilität des Unternehmens

  Ankerbeispiel:

  „Schliesslich [sic!] wurden die Umfrageteilnehmer auch bezüglich der Gesamtkapitalrendite (ROI) befragt. Hier gaben 59 Prozent der Ostschweizer KMU an, im letzten Geschäftsjahr eine Gesamtkapitalrendite von vier oder weniger Prozent erreicht zu haben" Quelle: Gossauer Nachrichten 09_10_2019, S.13

Nach der Gewinnung des entsprechenden Datenmaterials können die eigentlichen Auswirkungen der EUDSGVO für die einzelnen Bereiche Datenbank, Grafik-Software, Hosting und Development untersucht werden, konkret also welche Änderungen sich in den einzelnen Punkten ergeben

hinsichtlich der Kosten und Vorteile. Die entsprechende Untersuchungsmatrix ist nachfolgend in Tabelle 1 dargestellt.

	mit EUDSGVO	ohne EUDSGVO	mit EUDSGVO	ohne EUDSGVO	mit EUDSGVO	ohne EUDSGVO	mit EUDSGVO	ohne EUDSGVO
	Datenbank		Grafik-SW		Hosting		Development	
Cashflow	?	?	?	?	?	?	?	?
Verschuldensgrad	?	?	?	?	?	?	?	?
Personalkosten in Prozent der Betriebsleistung	?	?	?	?	?	?	?	?
Return on Sales	?	?	?	?	?	?	?	?
Return on Investment	?	?	?	?	?	?	?	?
Spalte und Summe der Felder mit besseren Werten	?	?	?	?	?	?	?	?
Ergebnis im Endeffekt	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-
Summe der + (positiv)	?							
Summe der - (negativ)	?							
Auswirkung daher	in Summe positiv oder negativ							

Tab. 1: geplante Auswirkungen (eigene Darstellung)

Für das Ergebnis sollen die einzelnen Teilergebnisse dahingehend einfließen, um entweder positive oder negative Auswirkungen einzutragen. Jedes Feld hat dabei die Wertigkeit 0 oder 1, wobei 0 für den schlechteren und 1 für den besseren Wert steht. Für den unwahrscheinlichen Fall, identische Werte sowohl mit als auch ohne EUDSGVO zu erhalten, wird in beiden Fällen der Wert 1 angenommen. Als Endergebnis werden die Spalten dann addiert und diejenigen Spalten mit mehr positiven Auswirkungen im Feld „Summe der + (positiv)“ sowie in jenem für „Summe der – (negativ)“ die negativen addiert. Die Differenz soll dann Aufschluss über entweder mehr positive oder negative Auswirkungen der EUDSGVO in Bezug auf das KMU im Bereich Webdesign- und –programmierung liefern.

2 Grundlagen

Mit der am 25.5.2018 in Kraft getretenen europäischen Datenschutzgrundverordnung (EUDSGVO) ändern sich viele Vorgehensweisen für Unternehmen, die Dienstleistungen auf dem Gebiet der Webprogrammierung erbringen und dabei Cloud-Services in Form von Storage sowie Infrastructure as a Service für ihre Kunden, also den Hosting-Bereich und Software as a Service für sich selbst zur Entwicklung nutzen. Anzumerken wäre, es hier mit Praktiken zu tun zu haben, die zwar weltweit eingesetzt werden, mit einem Schlag jedoch auf die EU im geografischen Sinn bezogen, illegal werden, sollte man die Bestimmungen der EUDSGVO ignorieren, was die einleitend erwähnten existenzbedrohenden, hohen Strafen nach sich ziehen kann (Art. 83 Abs. 5. EUDSGVO). Geschützt werden sollen personenbezogene Daten. Damit werden gleich zwei weitere Fragen aufgeworfen, nämlich was diese sind und wovor man sie schützen soll?

Kernpunkt jeglicher Datenverarbeitung sind zuerst einmal Datenerhebungen. Diese können durch Kunden in Form freiwillige Bekanntgabe oder durch zwangsläufige Erhebung zur Erfüllung eines Vertragsverhältnisses entstehen. Sie können allerdings auch automatisiert und oft ohne das Wissen Betroffener gesammelt werden, wie im weiteren Verlauf noch gezeigt wird. Besonders Letzteres erfordert Rechte auf Auskunft, Richtigstellung oder Löschung, was auch das Recht auf Vergessen werden beinhaltet. Es handelt sich um Regelungen die bisher in nationalen Datenschutzgesetzen geregelt waren, nunmehr jedoch auf europäischer Ebene Einzug gefunden haben (Art. 13 – 19 EUDSGVO).

Die Kernproblematik jeglichen Datenschutzes zielt daher auf den Schutz der Integrität (Integrity), Vertraulichkeit (Confidentiality) und Verfügbarkeit (Availability) ab. Dies bezeichnet man als CIA-Modell. Gemeint ist, die Daten in dem Sinne geheim halten zu können, sie vor fremden Zugriffen zu schützen. Sie müssen somit sicher vor Verfälschungen und auch verfügbar sein, womit der Schutz vor Ausfällen gemeint ist (Obernosterer, 2017, S.35). In jedem dieser Bereiche gibt es technische Möglichkeiten zur Verbesserung, allerdings auch menschliches Versagen, das zur Verschlechterung führen kann.

2.1 Technische Funktionen versus Datenschutz

Obige erste Frage lässt sich dahingehend beantworten, es immer dann mit personenbezogenen Daten zu tun zu haben, wenn die Rückführbarkeit auf eine konkrete Person möglich ist. Welcher Art diese Daten sind wird im weiteren Verlauf detaillierter behandelt. Ferner wird gezeigt, wo Grenzfälle bestehen, die es schwierig machen, Daten auf konkreten Personen zurückzuführen. Die Rede ist hier von anonymisierten und pseudonymisierten Daten, d.h. also, in dem Moment, wo z.B. die sog. Primärschlüsseln aus Datenbanken entfernt werden oder eindeutig rückführbare Merkmale wie z.B. Name und Adresse oder Telefonnummer, bzw. E-Mail-Adresse neutralisiert wurden. Ab diesem Zeitpunkt hat man zwar keine personenbezogenen Daten mehr, muss aber klassifizieren, ob sich diese nicht doch – wenngleich mit Aufwand – rückverfolgen lassen. Pseudonymisiert sind Daten, wenn man weitere Komponenten braucht, um diese wieder eindeutig Personen zuordnen zu können, anonymisiert dagegen, wenn dies nicht möglich ist (Gierschmann, Schlender, Stentzel, Veil, 2018, S.854 f.).

2.1.1 IP-Adressen und Logging

Die Kernproblematik der Identifizierbarkeit einer Person im Internet liegt in der IP-Adresse. Diese ist vergleichbar einer Absender-Adresse beim herkömmlichen Brief, bzw. einer Telefonnummer. Ruft man eine Webseite auf, muss die Gegenstelle zwangsläufig wissen, wohin diese übertragen werden soll. Und in dem Moment, wo etwas übertragen wird, lässt es sich auch abgreifen, z.B. mittels der Analysesoftware Wireshark. Das im Internet verwendete Protokoll TCP/IP macht dies möglich (Shaoqiang, DongSheng, ShiLiang, 2010, S.269). Im Gegensatz zur Rufnummernunterdrückung – außer für Sicherheitsbehörden - beim Telefonieren lässt sich eine IP-Adresse nicht unterdrücken. Würde man dies tun, endet die Verbindung. Während eine Telefonnummer einem konkreten Anschluss und somit auch normalerweise einem Gerät, bzw. Mobiltelefon zugeordnet werden kann, liegt die einzige Schwierigkeit bei einer IP-Adresse darin, den jeweiligen Provider schnell genug danach zu fragen. Im Detail geht es darum: eine Telefonnummer ändert sich

normalerweise nicht, außer bei Ummeldung, eine IP-Adresse dagegen praktisch ständig, v.a. beim IPv4-Protokoll. Der Grund liegt darin, einen knappen etwa 4 Mrd. Adressen umfassenden Raum weltweit für etwa 8 Mrd. Menschen und noch mehr internetfähige Geräte nutzen zu müssen.

Verwiesen sei hier auf das sog. NATting, also das Übersetzen von einer öffentlichen IP-Adresse in mehrere dahinter steckende Client-IP-Adressen im privaten Internet-Adressbereich. Diese Vorgehensweise hat historische Gründe, da mit den rund 4 Mrd. Internet-Adressen der Adressbereich knapp wurde und die Internet-Anbieter dazu übergehen mussten, Adressen aufzuteilen, indem diese für mehrere Endgeräte nutzbar gemacht wurden. Somit können sich öffentliche Internet-Adressen durchaus etliche hundert bis auch Millionen Personen gleichzeitig teilen, je nach Klasse A, B oder C-Netzaufteilung. Da es sich hierbei jedoch nicht um eine technische Arbeit handelt, sei auf die weiterführende Literatur hierzu verweisen. Hier ist von Interesse, zumindest beim Internet-Anbieter in Erfahrung bringen zu können, welchem Kunden zu welchem Zeitpunkt welche IP-Adresse zugewiesen wurde. Diese Daten benötigt der Anbieter meist zur Rechnungslegung bei Volume basierter Abrechnung oder auch zwecks Erfüllung staatlicher Speicherpflichten – erwähnt sei an dieser Stelle die Vorratsdatenspeicherung (Help.gv.at, 2019) zur Erhebung von Verbindungsdaten, wer wann welches Gerät kontaktiert hat, d.h. zwar nicht den Inhalt, jedoch Aufrufer und aufgerufene Gegenstelle.

Einfacher wird die Zuordnung bei statischen IP-Adressen, die der Provider an seine Kunden vermietet hat und noch einfacher bei IPv6, wenn rund 340 Sextillionen, d.h. 2 hoch 128 eindeutige Adressen zur Verfügung stehen. Damit könnte man jeder Person ein Leben lang eine eindeutige Internet-Kennung zuweisen (Ahmed, Asadullah, 2009, S.7). Doch selbst für IPv6 ist der Provider erster Ansprechpartner, wer denn nun konkret diese Adresse inne hatte beim Abruf einer Webseite.

Deutlich wird jedoch in allen Fällen, anhand einer IP-Adresse eine Person identifizieren zu können. Die EUDSGVO verlangt jedoch das genaue Gegenteil.

Es kommt nicht darauf an, zu wissen oder nicht zu wissen, wer hinter einer IP steckt, sondern auf die potentielle Möglichkeit, dies in Erfahrung bringen zu können. Erst wenn IP-Adressen anonymisiert vorliegen, d.h. also - um einen Analogieschluss zum Telefon zu ziehen - z.B. die letzten 3 Ziffern auszublenden. Bei IPv4 hieße dies das letzte Oktett einer IPv4-Adresse nicht zu speichern. Damit hat man sich jedoch ein neues Problem eingehandelt. Für Unternehmen im Bereich Webdesign ist es essentiell bei der Fehlersuche vollständige IP-Adressen in Logfiles zur Verfügung zu haben. Zu denken wäre etwa an Online-Banking-Lösungen, wo bestimmte IP-Bereiche gar keinen Zugriff erhalten sollen. Bei IPv6-Adressen bestehen Möglichkeiten die Privacy Extensions zu nutzen, wie in RFC 4941 spezifiziert. Im Kern geht es darum, auch bei IPv6 eine gewisse Dynamik einzubringen, indem das Präfix des Interface-Teils von Zeit zu Zeit zufällig wechselt (RFC, 2007, Nr. 4941).

Die im Internet verwendeten IP-Adressen werden, auch wenn sie dynamisch zugeordnet werden, laut Judikatur des EuGH schon seit 2016 als personenbezogen angesehen (EuGH, 19.10.2016 - C-582/14, 2016). Dies mag in der Praxis nicht immer eindeutig zuordenbar sein. Rechtlich jedoch wäre die nächste Problematik angesprochen. Das Loggen, also protokollieren von Datenzugriffen und Systemereignissen. Es stellt in der EDV kein Problem dar, faktisch alles in Ereignisprotokollen zu protokollieren, was primär dazu dient, Fehler zu finden oder auch Systeme und Software zu verbessern. Damit sind Telemetriedaten zur Nutzung gemeint. Genau dies birgt ein hohes Potential an möglichen Datenschutzverstößen in sich. Konkret lassen sich Zugriffe auf Webseiten, einzelne Datensätze von Datenbanken, Suchanfragen in Webmasken, Art der verwendeten Client-Systeme, Datum, Uhrzeit, gestartete und genutzte Software, System-Start- und Herunterfahr-Ereignisse, die öffentliche IP-Adresse, etc… protokollieren.

Heutige Betriebssysteme sind diesbezüglich sehr auskunftsfreudig, was Logfiles anbelangt, besonders was unixoide, also Unix, bzw. Linux-Systeme betrifft, von dem man als reiner Anwender nicht einmal eine Ahnung hat, dass etwas geloggt wird (Zeng, Xiao, Chen, 2015, S.7163). Während jedoch Linux quelloffen ist, ist

es Windows, das beim Logging den unixoiden Systemen in nichts nachsteht nicht. Die Problematiken hinsichtlich des Datenschutzes, die sich daraus ergeben, was Angriffe über Netzwerke mit dem Ziel Daten abzugreifen anbelangt, sind es konsequenterweise auch (Baraht, 2017, S.2).

Für ein Webdesign-KMU bieten sich hier v.a. Überraschungen bei Verwendung von Standardeinstellungen für Logfiles von Webservern wie Apache, den FTP-Services, oder bei Storage as a Service-Lösungen basierend auf der frei erhältlichen Owncloud- oder Nextcloud-Distributionen. Für die Details, was Linux, bzw. Windows alles protokolliert sei auf obige Literatur verwiesen. Interessant im Rahmen dieser Abhandlung ist dagegen, wie man Logfiles konform der EUDSGVO bekommt. Die Antwort fällt dabei eindeutig und kurz aus: man hat sie entweder zu deaktivieren, was nicht immer ein einfaches Unterfangen ist oder aber man weist Kunden auf die systembedingte Speicherung aller ihrer übermittelten Daten ihres Zugangsgerätes hin. Konkret lassen sich vom Kunden Typ, User-Agent, IP-Adresse, aus dieser sich auch die geografische Region, bzw. die Stadt des Internet-Providers ermitteln lässt, Speicherdauer, abgerufene Webseite, Eingaben in Formularfelder über sog. CGI-Interface-Schnittstellen oder Session-Cookies und dergleichen loggen. Letztere sind ein Beispiel dafür, wie man Datenschutz wahren kann. Wie der Name bereits sagt, verfallen diese Cookies nach Beendigung der Browser-Session. Der Vorteil: die Daten sind nicht gespeichert, der Nachteil: sie müssen neuerlich beim nächsten Besuch der Webseite eingegeben werden (Solmecke, Kocatepe, 2018, S.144). Das Problem dabei sind auch hier mögliche Angriffspunkte, denn Cookies lassen sich, wie bereits beim TCP/IP-Protokoll gesagt, auch unbefugt auslesen und verwerten (Sathiyaseelan, Joseph, Srinivasaraghavan, 2017, S.452).

2.1.2 Datenverknüpfungen ermöglichen Profilbildung

Werden Cookies, die technisch nichts anderes als eindeutige Kennungen sind, auf mehreren besuchten Webseiten durch betreibende Unternehmen ausgewertet, lassen sich eindeutige Nutzungs-Profile erstellen und die Kunden-Systeme mit zielgerichteter Werbung beim Webseiten-Aufruf ansteuern. Wird ein Online-Kauf getätigt, lassen sich die Systeme auch konkreten

Personen zuordnen – denn zwecks Lieferung von Waren sind Lieferadressen erforderlich. Diese Zusammenführung von Daten ermöglicht dann genaueste Informationen zur jeweiligen Person wie folgendes Beispiel zeigt:

Besucht man eine Webseite, die Babybekleidung anbietet und hinterlässt bei einer Bestellung Name und Anschrift, „weiß" die nächste Webseite, die z.B. mit Autoartikeln handelt und ein entsprechend hinterlassenes Cookie auswertet mit fast sicherer Wahrscheinlichkeit, die hinter dem Client-System steckenden Person könnte auch an Kindersitzen interessiert sein. Das Ganze nennt sich Data-Mining. Beispiele für solches Data-Mining sind die Big Player am Markt wie Google, Amazon und Ebay sowie v.a. soziale Netzwerke wie Youtube und Facebook. Teilweise können an letztere Dienste auch Daten übertragen werden, ohne überhaupt dort registriert zu sein. Dazu ist es ausreichend, im Internet z.B. seine Telefonnummer oder E-Mail-Adresse anzugeben, die über die vorhin genannten Cookies lediglich durch Aufruf einer Webseite, die aus technischer Sicht einen sog. IFRAME verwendet und darin Content von Facebook darstellte, die Daten an das soziale Netzwerk übertrug. War nun ein Bekannter bereits registrierte Kunde von Facebook und hatte dieser sein Adressbuch von seinem Mobiltelefon über die Facebook-App zugänglich gemacht, konnte Facebook auch in weiterer Folge die Spuren der so ermittelten Person auswerten, den Namen konkret zuordnen und für eigene Marketing-Zwecke nutzen. Damit werden v.a. zwei Probleme deutlich: einerseits die Erhebung und Verwendung sowie die Weitergabe, bzw. Übertragung von Daten. Besonders Facebook betreffend machte der Fall Cambridge Analytica Schlagzeilen, wo 87 Mio. Datensätze ausgewertet wurden und aktiv zur Beeinflussung der Wählerschaft im US-Wahlkampf 2016 verwendet wurden (ORF Online 3, 2019).

2.2 Modifikationszwang von Webseiten: soziale Netzwerke

Obige Probleme sind der Grund, warum seit dem Inkrafttreten der EUDSGVO Änderungen im Webdesign erfolgen mussten und zwar dahingehend, bewusst bereits im Vorfeld für Aktivierung der Datenübertragung an soziale Netzwerke durch einen Zustimmungsbutton sorgen zu müssen. Auch gibt es kaum noch Webseiten, die nicht entsprechende Hinweise einblenden, wo man Cookies

ebenfalls zustimmen muss, widrigenfalls die Funktionalität der Webseite auch hier entweder gar nicht oder nur eingeschränkt ermöglicht wird. Problematisch in diesem Zusammenhang ist das sog. Kopplungsverbot, das noch behandelt wird. Dazu ist anzumerken, bei Cookies es nicht immer mit Data-Mining, sondern auch mit durchaus legitimen Zwischenspeicherungen der erwähnten Session-Cookies zu tun haben zu können. Damit ist gemeint, zwischen dem Wechsel von Webseiten z.B. eingegebene Daten auch auf die nächste Seite mit zu übernehmen, was technisch durch die Server im Hintergrund erfolgt. Da auch hier eine Zwischenspeicherung vorliegt und damit Daten verarbeitet werden, braucht es auch hier zuerst die Einwilligung (Art. 13 und 14. EUDSGVO). Eindeutige Aussagen, was nun von welcher Webseite durch Cookies gespeichert wird, lassen sich an dieser Stelle nicht treffen. Dazu ist die Spanne an Angeboten und der Ausrichtung der Webseiten betreffend deren Zielgruppen zu umfangreich. Entsprechenden Hinweise sollten grundsätzlich gelesen und - darin besteht die Gefahr - nicht einfach aus Gewohnheit künftig weggeklickt werden. Die Folgen können, zu den erwähnten Datenübertragungen führen.

Damit wäre an dieser Stelle die oben aufgeworfene zweite Frage bereits einfacher zu beantworten, wovor man denn seine Daten schützen müsse? Die Antwort lautet: man schützt seine Daten vor Missbrauch und kommerzieller Verwertung zur Wahrung der informellen Selbstbestimmungsrechte. Ansonsten hat man mit Wildwuchs bei E-Mail-Spam, Direktmarketing-Werbeanrufen, gezielter Werbung im Postfach und Meinungsumfragen oder sogar mit Identitätsdiebstahl zu rechnen. Zwar könnte man meinen E-Mail-Spam zu löschen – Software unterstützt hierbei sogar durch Spam-Filter, ohne Eingabe seiner Kredit- oder Kontodaten samt Verifizierungscode könne ohnehin niemand etwas im Internet bestellen – von Sicherheitsrisiken und Softwarefehlern einmal abgesehen, denn diese sind nicht Gegenstand der Arbeit, bei Werbeanrufen von Direkt-Marketing-Unternehmen kann man einfach auflegen und klassische Briefwerbung in den Müll werfen. Ja, man kann. Dennoch ist dies mit Tätigkeiten verbunden, die im Büro Arbeitszeit kostet oder im Privatleben Freizeit. Meinen könnten man auch, der Aufwand der Verfolgung derartiger Anbieter, die

unverlangt mit jemandem in Kontakt treten, lohne sich nicht. Teilweise mag dies richtig sein, da diese mehrheitlich aus Drittstaaten wie China, USA und Vietnam agieren (Suhr, 2019) und in diesen greift die EUDSGVO ohnehin nicht wirksam. Auch nach dem Inkrafttreten der EUDSGVO zeugt der Anteil mit etwas mehr als 50% Spam-Mails deutlich davon, der bis Dezember 2018 trotz gegenteiliger Erwartung wieder auf 57% angestiegen ist (Statista, 2019). Interpretieren lässt sich dies nur so, die Strafen der EUDSGVO nicht zu fürchten, oder in Staaten zu sitzen, die entweder keinerlei Rechtshilfeabkommen oder großvolumige Handelsgeschäfte mit der EU tätigen, um Sanktionen zu fürchten.

Angesichts der hohen Strafen der EUDSGVO reicht es ansonsten, wenn nach und nach Unternehmen, die Datenmissbrauch betreiben, vom Markt gedrängt werden, um es milde auszudrücken. Deutlich wird dies anhand von Imageschäden. Unternehmen, die sich nicht an die EUDSGVO halten, haben entsprechend mit einem Rückgang ihres Auftragsvolumens zu rechnen. Solmecke et al. sprechen in diesem Zusammenhang auch vom „Abstrafen durch Kunden“ (2018, S.24). Insofern darf man gespannt auf Selbstregulierungsmechanismen blicken als es wohl nicht immer die Datenschutzbehörden brauchen wird, um mittels Sanktionen gegen unbeugsame Unternehmen vorzugehen. Das Drohende existenzielle Aus droht allerdings von zwei Seiten, nämlich den Behörden wie auch dem Markt, da bekanntlich ohne Nachfrage nach Produkten eines jeglichen Unternehmens dieses zwangsläufig in Konkurs geht. Außer Acht bleiben an dieser Stelle natürlich organisierte Verbrecher, die in Drittstaaten sitzen und selbst kein Unternehmen leiten, stattdessen Spam-Dienste anbieten oder in eigenem Interesse verfolgen. Auch hier wird man künftig auf die Behörden des jeweiligen Staates angewiesen sein. Handelt es sich allerdings um Staaten mit schlechtem Ruf – ohne diese beim Namen zu nennen – wird man weiterhin auf Software und den Hausverstand bezüglich Datenschutz setzen müssen. Ohne internationale Verträge mit diesen Staaten und dem Verfolgungswillen dort, wird sich auch hier nicht viel ändern.

2.3 Die Haupttätigkeitsbereiche beim Webdesign

Im Jahr 2017 verfügten 72% aller Unternehmen, also fast 3/4 über eine eigene Webseite (Solmecke et al., 2018, S.17). Damit wird das Potential deutlich, im Bereich Webdesign mit einem Zuwachs an Umrüstungsaufträgen durch diese rechnen zu können, um zur EUDSGO compliant zu werden. Die Haupt-Tätigkeitsbereiche von KMUs in diesem Bereich bewegen sich in den Bereichen Programmierung, Datenbanken, Grafik und Hosting. Für die vorliegende Arbeit werden Spezialfälle wie individuelle Anpassungen von Content Management Systemen (CMS) außer Acht gelassen. Generell lassen sich für jeden einzelnen Bereich derartige Spezialfälle konstruieren, beschränkt wird die Betrachtung jedoch auf die grundlegenden Erfordernisse für ein CMS. Typische Vertreter davon wären z.B. Typo 3, Wordpress, Joomla und Prestashop. Allen diesen Systemen gemein ist, eine Datenbank zu benötigen, dem Endanwender die Möglichkeit zu geben, selbst Content zu erzeugen und dabei offen für Erweiterungen durch Programmierung sind. Dies geschieht mittels Plugins oder direkter Änderung am Programmcode. Grafische Änderungen an den sog. Vorlagen, d.h. der Templates werden ebenfalls unterstützt und preislich kosten diese Systeme als Open Source-Anwendung nichts. Preislich gesehen fallen daher lediglich die Kosten der Modifikationen an - entweder am Code, dem Design oder bei der individuellen Implementierung in Form des Hostings.

Datenschutzrechtlich nach der EUDSGVO relevant sind dabei die Möglichkeiten, die CMS-Systeme an neue Gegebenheiten anzupassen. Genau darin liegen auch geringe Kosten begründet. Ist ein CMS einmal an die EUDSGVO angepasst, dient dies als Vorlage für sämtliche weiteren Aufträge durch Kunden. Konkret ist damit ein einmaliger Aufwand verbunden, entsprechende Plugins zu entwickeln, was allerdings die Community durchführt und auch hier nicht das Webdesign-KMU selbst erledigen braucht. Damit fallen auch hier Kosten weg. Was bleibt, ist lediglich der Aufwand der Implementierung. Dies kann dabei im operativen Tagesgeschäfts miterledigt werden und bedeutet nicht mehr Aufwand als z.B. der Kundenansturm zu Weihnachten und Ostern im regulären Handelsverkauf. Um es auf den Punkt zu bringen hält sich die Anpassung von

CMS an die EUDSGVO daher in bescheidenen Grenzen, weshalb diese Kosten mit 0 angesetzt werden können. Dagegen ist mit Mehreinnahmen beim Webdesign-KMU für die Adaptierung bestehender Systeme bei dessen Kunden in der entsprechenden Anzahl zu rechnen, während ohne EUDSGVO dem Tagesgeschäft nachzugehen wäre, also Business as usual, in der Hoffnung auf Neukundengewinn. Insofern erfordert die EUDSGVO – einmal mehr - eine Änderung bestehender Webseiten und Datenbanken, wie bereits zuvor die Impressumspflichten, das Verbot von Werbung für Ärzte, Umsetzung der E-Commerce-Richtlinie und den Informationspflichten über Rücktritte bei Online-Geschäften. Anders ausgedrückt, werden Unternehmen im Bereich Webdesign häufig mit geänderten Rechtslagen konfrontiert, die ihnen Aufträge bescheren.

2.4 Die EUDSGVO: Kernpunkte im Detail

Was nun die zentralen Änderungen der EUDSGVO für Unternehmen bedeutet, lässt sich in sechs Prinzipien einteilen (Gobeo, Connor, Buchanan, 2018, S.14ff), nämlich

Prinzip 1: Gesetzmäßigkeit, Fairness und Transparenz

Alle Daten müssen gesetzmäßig erfasst sein und einem der folgenden sechs Zwecke dienen. Fairness bedeutet Betroffenen Selbstbestimmungsrechte einzuräumen, welche Daten, wann, ob und wie sie erfasst werden, was auch Änderungs-, Berichtigungs- und Löschwünsche beinhaltet. Transparenz beinhaltet die Informationspflicht gegenüber Betroffenen, bevor die Verarbeitung beginnt, d.h. also z.B. mittels Cookie-Hinweise oder Einwilligungen zur Übertragung an soziale Netzwerke im Vorfeld auf die Datenspeicherung und Übertragung hinzuweisen.

Die Zwecke wären:

- Einwilligung des Betroffenen - z.B. Gewinnspiele
- Errichtung eines Vertragsverhältnisses - z.B. Dienstleistungsvertrag beim Webdesign-KMU

- gesetzliche Verpflichtung - z.B. Aufbewahrungsfristen für Rechnungslegungen und Gewinnversteuerung, etc...
- lebensrettende Maßnahmen - z.B. Auskunft über medizinische Daten wie Allergien und Medikamente
- behördliche Interessen - z.B. Melderegister, Strafverfolgung bei KFZ-Kennzeichenabfragen
- besondere Interessen - d.h. für alle Organisationen, die keine staatlichen Behörden sind - z.B. Umfragen und statistische Erhebungen

Prinzip 2: Zweckbindung

Daten dürfen nur für den erhobenen Zweck verwendet werden und bedürfen bei darüber hinausgehender Verwendung der Einwilligung Betroffener. Genau dieser Punkt wird oft v.a. beim Adresshandel oder der Verknüpfung von Daten durch soziale Netzwerke nicht beachtet.

Prinzip 3: Datenminimierung

Es dürfen nur Daten, die zur Erreichung des Verarbeitungszweckes erforderlich sind, erhoben werden. So sind zur Rechnungslegung und den Bankeinzug Name, Anschrift und Kontodaten einer Person erforderlich. Telefonnummer sowie E-Mail-Adresse dagegen sind hingegen für eine derartige Transaktion nicht mehr erforderlich, können allerdings unter Hinweis auf Freiwilligkeit und zwecks besserer Kundenkommunikation abgefragt werden. Der Zweck ist dann eben diese „verbesserte Kundenkommunikation". Keinesfalls aber dient diesem Zweck dann die Abfrage z.B. nach der Anzahl der Kinder.

Prinzip 4: Richtigkeit

Daten müssen richtig sein, bzw. dort wo dies nicht der Fall ist ehestmöglich berichtigt werden. Betroffene haben auch das Recht auf Richtigstellung.

Prinzip 5: Speicherdauer

Daten dürfen nicht länger als für den vorgesehenen Zweck gespeichert werden. Endet z.B. ein Vertragsverhältnis, dürfen über die gesetzlichen Speicherverpflichtungen hinaus die Daten nicht gespeichert werden.

Prinzip 6: Integrität und Vertraulichkeit

Daten dürfen nicht verfälscht sein und müssen vertraulich behandelt werden.

Besonders beim letzten Punkt ist das Webdesign-KMU gefordert, nur verschlüsselte Kommunikation anzubieten, also dem Stand der Technik entsprechend SSL-Zertifikate einzusetzen sowie sich von Schutzmaßnahmen beim Hoster zu überzeugen, bzw. diese selbst zu implementieren, was virtuelle Systeme anbelangt und auch dessen sowie eigene Firewall-Systeme für den Unternehmenssitz einzusetzen. Gehashte Passwörter und auch 2-Faktoren-Authentifizierung sollten ebenfalls verwendet werden.

Was Informationssysteme anbelangt, bestehen Werte im Unternehmen nicht nur aus Hard- und Software, sondern auch in Verfahren und Personal (Gobeo et al., 2018, S.71f.), außer, wenn Cloud Services egal ob IaaS, PaaS oder SaaS in Anspruch genommen werden. Assets des Unternehmens müssen früher oder später outgesourced werden, wenn seitens der Hersteller keine on-premises-Lösungen mehr angeboten und supported werden. Adobe bietet z.B. für das hier betreachtete Webdesig-KMU seine Creative Suite nur mehr als Software as a Service-Lösung an. Es bleiben also Verfahren und die Daten, die vielfach als das Öl der Zukunft angesehen werden. Denn während Hard- und Software, sowie Personal jederzeit ersetzbar sind, sind es die Daten und Verfahren nicht. Sind diese verloren und hat man kein Backup, droht das existenzielle Aus. Ein bekanntes Opfer wurde der für die US-Raumfahrtbehörde NASA tätige Zulieferer Omega Engineering. Täter war der eigene Systemadministrator. Dieser schleuste aus Rache für seine Entlassung nach mehreren Jahren beim Unternehmen einen Überschreibbefehl in den zentralen Server ein und vernichtete auch das einzige Backup-Band. (Forensic Files, 28.04.2019 - 1:20h). Mit einer Storage as a Service-Lösung wäre dies bei zwei redundanten Anbietern

mit jeweils einem eigenen Systemadministrator, der nur die Zugangsdaten zu „seinem“ Anbieter kennt, nicht passiert.

3 Related Work

Erwähnt wurde bereits die Gefahr der Datensammlung in modernen Betriebssystemen. Dieses Wissen ist bereits bekannt, jedoch erfordert es erst im Zuge der EUDSGVO neue Herangehensweisen und Umrüstungsmaßnahmen, will man nicht Gefahr laufen durch veraltetet Hard- und Software mit den erwähnten Strafsanktionen rechnen zu müssen.

3.1 Telemetrie- und Diagnosedaten in Software

Was Diagnosedaten anbelangt, können damit potentiell Bereiche des Hauptspeichers und damit auch dessen Inhalt an den Hersteller übertragen werden. Besonders erwähnenswert ist hier Windows 10. Wie das deutsche Bundesamt für Sicherheit in der Informationstechnik herausgefunden hat, lassen sich Telemetriedaten des Systems lediglich in der Enterprise-Version auf 4 Verbindungen reduzieren. Tabelle 2 veranschaulicht das Ergebnis:

Telemetrie-Level	aufgebaute Diagnosedaten-Verbindungen an den Hersteller
Security	4
Basic	410
Enhanced	418
Full	422

Tab. 2: Telemetrie in Windows 10 (BSI, 2018, S.24)

Eine Komplett-Abschaltung lässt sich nur durch Deaktivierung eines Dienstes und Setzen eines Wertes in der Registrierdatenbank erreichen – ein Unterfangen also, das für die Mehrzahl nicht technik-affiner Personen unmöglich sein dürfte.

Exkurs: Windows 10 – Telemetrie deaktivieren:

Der Dienst „Benutzererfahrung und Telemetrie im verbundenen Modus“ gehört unter den laufenden Diensten → Start / Ausführen: „services.msc“ vom Starttyp automatisch auf deaktiviert gesetzt und auch beendet. In der sog. Registry muss zudem unter dem Schlüssel HKLM\SYSTEM\CurrentControlSet\Control\WMI\Autologger\AutoLogger-DiagTrack-Listener der Wert von „Start“ auf 0 gesetzt werden. Windows gehört anschließend neu gestartet.

Auch das niederländische Justizministerium kommt zum Schluss, dass Hersteller Microsoft nicht nur mit Windows 10, wie oben gezeigt wurde, sondern auch mit den Office-Suiten in den Versionen 2013 und 2016 hinsichtlich der

Diagnosedaten, die standardmäßig nicht deaktivierbar sind, gegen die EUDSGVO verstößt.

„The transfer of data is a risk in itself. As has been explained above, in the paragraph about the identification of the risks, diagnostic data reveal behavioral information about employees and other people in the Netherlands that communicate with these employees. The diagnostic data may also include parts of the content of documents when using Connected Services and subject lines from e-mails. This leads to a high risk of serious harm, especially when the collected data (inadvertently) include special categories of personal data, and classified information." (Nas, Roosendaal, S.81)

Schon alleine der Umstand hier überhaupt Daten zu übertragen wird als Sicherheitsrisiko eingestuft. Waren es bei Windows 1.000 - 1.200 Ereignisse, übertrifft Office mit 23.000 - 25.000 Ereignisarten diesen Wert um fast das 21-fache (Nas, Roosendaal, 2018, S.5). Wesentlich dabei ist, Office auch auf älteren Windows-Versionen einsetzen zu können und damit auch Daten von Anwendern zu verarbeiten, die noch gar nicht auf Windows 10 upgedated haben. Zudem ist es unwahrscheinlich, den Programmcode von Office, der über mittlerweile Jahrzehnte seit Windows 3.0-Zeiten Anfang der 90er-Jahre des letzten Jahrhunderts gewachsen ist, in wenigen Monaten reengineeren zu können und alle Sammelroutinen daraus zu tilgen. Dies mag zwar Spekulation sein, die Zukunft wird jedoch zeigen, ob dies zutreffend ist oder nicht.

3.2 Warum ist die Telemetrie für Webdesigner relevant?

Für Webdesigner ist Telemetrie von Software insofern relevant, als z.B. etliche Dokumente in Word und Excel unter Windows als Quasistandard verfasst werden und auf Webseiten zum Download angeboten werden – PDF dient dagegen mehr der Archivierung und gleicher Darstellung des Inhaltes auf den jeweiligen Ausgabegeräten (Zhao, 2011, S.371). Jedenfalls hat das hier betrachtete Webdesign-KMU dieses Format schon alleine aus Gründen der möglichen Datenanlieferung durch dessen Kunden über die MS-Office-Suite zu unterstützen, auch in Hinblick auf Kompatibilitätsprobleme, sollte es stattdessen reine Open Source Produkte verwenden wie Open- oder Libre Office. Dadurch stellt sich auch hier die Frage, wenn Kundendokumente geöffnet werden, welche Daten auf MS-Server übertragen werden. Einer Auswertung dieser Telemetriedaten widersprechen kann man nämlich nicht (Nas, Roosendaal, 2018,

S.36), was per se neuerdings nicht mehr EUDSGVO-konform ist. Dies widerspricht jedoch dem sog. Kopplungsverbot (Art. 7 Abs. 3 EUDSGV). Damit ist gemeint, ein Produkt nutzen, allfällige Datensammlungseinwilligungen jedoch freiwillig abgeben zu können. Eine Voraussetzung zur Nutzung des Produktes darf nicht davon abhängig sein, Datensammlungen zustimmen zu müssen oder noch schlimmer automatisiert und unwissentlich zur Verfügung zu stellen. Interessant in diesem Zusammenhang sind auch moderne Smartphones. Diese beinhalten teilweisen Nutzungsklauseln, denen zugestimmt werden muss, widrigenfalls sich das Gerät ebenfalls nicht, bzw. zumindest nicht in vollem Umfang nutzen lässt.

3.3 Der rechtliche Aspekt

Vorweg: rechtliche Aspekte sind nicht Gegenstand dieser Arbeit und werden daher nur kurz, jedoch mit den zentralen Problemen hinsichtlich der EUDSGVO behandelt. Es geht darum, wie vorhin angeführt, Datensammlungen im elektronischen Verkehr durch entsprechende Hard- und Software zu beschränken. Das Problem ist jedoch, den Lizenzverträgen in der Regel erst nach deren Kauf durch sog. Klick- oder Touch-Wrap-Verträge am Bildschirm zustimmen zu müssen. Ohne Zustimmung ist grundsätzlich keine Nutzung möglich. Datenschutzrechtlich relevant ist hier jedoch, es mit Produkten zu tun zu haben, durch die eine –wenngleich rechtlich unwirksame - Zustimmung zu Nutzungsverträgen, trotzdem mit dem Sammeln und Aufzeichnen des Nutzerverhaltens einhergeht – die Software „weiß“ ja nicht, dass „sie nicht darf“.

Man hat es ja in der ständigen Rechtsprechung mit eindeutig ausjudizierten Fällen zu tun, nämlich der Unwirksamkeit nachträglicher oder überraschender Nutzungsklauseln, bei deren Nichtzustimmung keinerlei Nutzung des Gerätes oder der Software möglich ist, eben das angesprochene Kopplungsverbot. Bezogen auf obige Erkenntnis mit den Office-Produkten und Smartphones oder auch mobilen Endgeräten für die Webseiten in Zeiten des Internet of Things immer wichtiger werden, kann das hier betrachtete KMU gar nicht dem Wunsch von Kunden entsprechen, eine allfällige Weiterverarbeitung von Daten zu unterlassen. Es kann auch nicht wissen, welche Daten, sollte es Windows 10-

Geräte oder v.a. Android-Smartphones hinter denen Google steckt, zwecks Test der entwickelten Webseiten, nutzen, an den Hersteller übertragen werden. Die Hersteller dieser Produkte sind dagegen als Auftragsverarbeiter im Sinne des Art. 28 EUDSGVO anzusehen und mit diesen einen Sondervertrag abzuschließen wird in der Regel an der zahllosen Anzahl der Nutzer dieser Produkte – d.h. Standardsoftware und Massenhardware – scheitern.

Eingestehen muss man jedoch, dass es um Geräte und Software geht, die schon vor dem Inkrafttreten der EUDSGVO verfügbar waren oder bereits entwickelt wurden und nun nicht compliant auf dem Markt ist. Mittels allfälligen Patches oder genereller Deaktivierung der Datensammlungsroutinen ist man jedoch zögerlich, wohl auch deswegen, da ja bereits den Aufklärungsgeboten (Art. 13 und 14 EUDSGVO) entsprochen wird, wenn auf die Datenverarbeitung hingewiesen wird, was ja meist auch der Fall ist. Somit handelt es sich nicht um einen Nutzungsvertrag im urheberrechtlichen Sinne, sondern um einen Hinweis wie bei Cookies, eben Daten zu erheben und zu verarbeiten. Verschärft werden soll jedenfalls das Cookie-Management durch die ePrivacy-Verordnung. In einem offenen Brief an den deutschen Bundesminister für Wirtschaft und Energie, Peter Altmaier, fordern diverse NGOs ein beschleunigtes Konkretisieren und Inkrafttreten der ePrivacy-Verordnung, da bisher auf europäischer Ebene nach wie vor Uneinigkeit über die konkrete Ausgestaltung herrscht u.a.:

„Deutschland muss seine Arbeit intensivieren, gegen die aufdringlichen und missbräuchlichen Praktiken auf dem digitalen Markt vorzugehen, die das Recht auf Privatsphäre, Meinungsfreiheit und Datenschutz verletzen und zudem Vertrauen, Innovation und die Nutzung neuer Dienste beeinträchtigen.“ (offener Brief diverser NGOs an den deutschen Bundesminister für Wirtschaft und Energie, 2018)

Treffender kann man es nicht ausdrücken. Denn genau dieses Vertrauen ist es ja letztlich, das zu zögerlichem Umgang mit Cloud-Anbietern führt. Sicherheitsrisiken, Zuverlässigkeit des Anbieters und das Verhältnis zu diesem, was Abhängigkeit inkludiert, wären an dieser Stelle zu nennen (Abdoulaye, 2014, S.33). Was Webseiten betrifft, reichen jedenfalls bloße Cookie-Hinweise ab dem Inkraftreten der ePrivacy-Verordnung – geplant war sie eigentlich noch

2019 – nicht mehr. Jedwedes Gerät muss hier standardmäßig voreingestellt werden, Cookies nur explizit zuzulassen, also ein Opt-In bieten (WKO, 2017, S.53). Derzeit ist es noch so, im Zuge des Komforts beim Surfen im Internet, Cookies zugelassen zu haben, weshalb der Aufklärungspflicht der EUDSGVO Genüge getan werden muss und im Vorfeld des Setzens von Cookies darauf hingewiesen wird. Mit der ePrivacy-Verordnung dürfen Cookies standardmäßig gar nicht funktionieren, bis sie aktiviert sind, was bedeutet, hier mit vielen Aufträgen an Webdesigner rechnen zu können, Seiten auch dahingehend umzuprogrammieren, dass diese auch ohne Cookies funktionieren.

Deutlich wird damit die Problematik obiger veralteter Software aus Zeiten vor der EUDSGVO oder ePrivacy-Verordnung, wie obige Untersuchung der Niederlande zeigte. Beide MS-Office Produkte in den Version 2013, 2016 sowie Windows 10 von 2015 stammen ja aus Zeiten vor Inkrafttreten der EUDSGVO im Jahr 2018. Regelungen wie nun damit umzugehen ist, existieren nicht, da jedoch alle Personen sowohl juristische wie private, die Daten verarbeiten, von der EUDSGVO betroffen sind und auch schon ihre Unternehmensprozesse adaptieren mussten, ist davon auszugehen, auch Hersteller von Software, die nicht EUDSGVO-konform arbeitet, rechtlich verfolgen zu können. Denn: wenngleich die Software Daten sammeln möge, so obliegt es letztlich dem Hersteller die Daten tatsächlich auch auf seinen Servern in Empfang zu nehmen. Da nicht bekannt ist, dass Microsoft die Datenverarbeitung eingestellt hat, fällt deren Verarbeitung unter die EUDSGVO - und damit liegen mit hoher Wahrscheinlichkeit Verstöße vor. Eine rechtskräftige Höchstgerichtentscheidung dazu ist jedoch noch nicht bekannt.

Ähnlich verhält es sich mit Diagnosedaten in Fahrzeugen. Kauft man heute ein modernes Auto, kann man dieses nur nutzen, wenn man einen Vertrag mit dem Hersteller abschließt, diesem die Diagnosedaten des Fahrzeuges zur Verfügung zu stellen. Problematisch wird dies, wenn das Fahrzeug eines Tages veräußert werden sollte. Der Gebrauchtwagenkäufer hat nämlich keinen Vertrag mit dem Hersteller zur Überlassung der Diagnosedaten. Wenn auch dieser nicht mit der weiteren Sammlung von Daten einverstanden ist, sendet das Fahrzeug trotzdem

die Diagnosedaten. Hier muss der Käufer also von einem Widerspruchsrecht der EUDSGVO gebraucht machen für Daten, deren Verwendung er eigentlich gar nicht zugestimmt hat. Die Problematik des sog. Sekundärmarktes bietet daher ebenfalls reichlich Betätigungsfeld für juristische Auseinandersetzungen. Denn sicher ist eines: anhand der Diagnosedaten lassen sich mittels GPS die Position des Fahrzeuges und damit das Nutzungsverhalten bestimmen. (Elamin, Wadah , Elwasila, Abdallah, Alkasim, 2018, S.3)

Deutlich wird an dieser Stelle, bestehenden Unternehmen zwar die Verpflichtung auferlegt zu haben, die bis dahin gültigen Verfahren und Business Prozesse EUDSGO-konform zu adaptieren, obige Beispiele zeigen jedoch, welche Probleme es auf dem etablierten Massenmarkt für Massenprodukte wie eben bisheriger Standard-Software und allgegenwertige Smartphones und Autos gibt. Ist man sich hier nicht sicher, welches Produkt welche Daten wann und wohin überträgt, trifft es auch Anbieter wie Webdesign-KMUs, die Daten ihrer Kunden erfassen müssen, Daten, die dann auch zu den Herstellern der Bürosoftware, hier Microsoft, der verbreiteten Smartphones mit dem Betriebssystem Android – also Google – oder den Autohersteller transferiert werden. Moderne Schnittstellen in Fahrzeugen machen es zudem möglich mittels USB- und Bluetooth Geräte einzubinden, womit man auch hier bei der EDV angelangt wäre und Daten der jeweiligen Geräte an die Hersteller der KFZ übertragen kann.

Allerneuerste Software und Hardware bietet dabei tatsächlich Einstellungen, die gemäß Privacy by Design und Privacy by Default der EUDSGVO genügt, weshalb an dieser Stelle doch schon einen Umdenkprozess eingeleitet wurde, wohl auch in Hinblick auf schlechte PR-Wirkung. Allerdings muss betont werden, derartige Geräte nur im EU-Raum entsprechend vorkonfiguriert ausliefern zu müssen. Einer Datensammlung z.B. auf dem US-Markt durch dortige Software, Smartphones oder Fahrzeugen steht weiterhin nichts im Wege.

Für das hier betrachtete Webdesign-KMU stellt sich die Frage nach der Vermeidung der einleitenden existenzbedrohenden Strafen. Angesichts dieser ist es keine Schande, Experten in Anspruch zu nehmen, sei es in Form von

Rechtsauskünften, Anwälten oder seitens behördlicher Unterstützung. Dies ist dann als Investition für Compliance anzusehen, welche Kosten hinterher spart (Solmecke et al., 2018, S.28), v.a. bezogen auf Schadenersatz und Unterlassungserklärungen in den Mitgliedsstaaten der EU. Große Unternehmen verfügen ohnehin meist über eigene Rechtsabteilungen. Generell sind Versicherungen angesichts der Komplexität der Materie und Haftungen anzuraten. Die Versicherungssumme sollte den existentiellen Wert des Unternehmens abdecken. Wie Kurbos schon 1999 wusste, kommen an dieser Stelle neben Geräteausfallsversicherungen, auch Betriebsunterbrechungs-, Haftpflicht, Vermögens- und v.a. Rechtsschutzversicherungen in Frage (1999, S.128ff.). Konkret bedeutet dies, bei den Auswirkungen der EUDSGVO auch auf bestehende Ressourcen zugreifen zu sollen, um Haftungsrisiken zu vermindern. Selbst für KMUs, die juristisch völlig schutzlos und ohne Beratung dastehen, bietet die Wirtschaftskammer Österreich diverse kostenlose Praxisinfos, Umsetzungsinformationen und behördliche Musterdokumente zum Download an ebenso wie das IT-Sicherheitshandbuch für KMUs und Mitarbeiter. Auch das IT-Grundschutzkompendium des deutschen Bundesamtes für Informationssicherheit ist empfehlenswert. Die Ressourcen finden sich unter:

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2018.pdf?__blob=publicationFile&v=9
- https://www.ots.at/presseaussendung/OTS_20180219_OTS0028/umsetzung-der-dsgvo-neues-kostenloses-serviceangebot-der-wkoe-bundessparte-handel
- https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationen-zur-EU-Datenschutz-Grundverordnung.html
- https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Musterdokumente-zur-EU-Datenschutzgrundverordnung.html
- https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html
- https://www.ots.at/presseaussendung/OTS_20180219_OTS0028/umsetzung-der-dsgvo-neues-kostenloses-serviceangebot-der-wkoe-bundessparte-handel
- https://www.wko.at/site/it-safe/sicherheitshandbuch.html
- https://www.wko.at/site/it-safe/mitarbeiter-handbuch.html

Damit lassen sich faktisch alle wesentlichen Anforderungen der EUDSGVO umsetzen, alleine indem man sich in die Materie einliest.

Hinsichtlich des Bestehens von nationalen Gesetzen neben der EUDSGVO finden sich entsprechende Problematiken der Rechtsauslegung auch für Deutschland bei Solmecke et al. (2018, S.19) Insofern wird deutlich, je mehr einheitliche Regelungen es für den digitalen Raum auf EU-Ebene noch geben wird, desto rechtssicherer werden binnenstaatliche Rechtsgeschäfte als auch solche die Kunden aus Drittstaaten mit nationalen Agenturen innerhalb der EU abschließen. Zu erwähnen wäre an dieser Stelle die besagte, aber noch ausständige ePrivacy-Verordnung, die der Achtung des Privatlebens und dem Schutz personenbezogener Daten in der elektronischen Kommunikation dient, d.h. damit auch hier für einheitliche Regelungen in der EU zu sorgen. Leider wird genau dies bekanntlich in der öffentlichen Wahrnehmung als zu viel EU-Zentralismus und Regelungswut kritisiert, wie z.B. durch den mittlerweile ehemaligen österreichischen Bundeskanzler Sebastian Kurz, was diesbezüglich von Noch-EU-Kommissionspräsident Jean-Claude Juncker dementiert wurde (Mayer, 2019). Solmecke et al. weisen jedoch zu Recht auf Problematiken hinsichtlich der EUDSGVO hin, da die ePrivacy-Verordnung Regelungen der EUDSGVO weiterhin konkretisieren oder sogar umkehren könnte (2018, S.19). Investitionen in umprogrammierte Webseiten wären dann seitens der Auftraggeber vergeblich gewesen. Als Webdesign-KMU hat man jedoch durch die EUDSGVO und ePrivacy-Verordnung volle Auftragsbücher zu erwarten.

Hinsichtlich der Problematiken geht es um sog. Öffnungsklauseln. Es ist jedoch anzumerken, es mit sehr vielen Öffnungsklauseln zu tun zu haben, d.h. im Endeffekt wird den Mitgliedsstaaten in vielen Bereichen der EUDSGVO weiterhin die Möglichkeit zur nationalen Regelung von Ausnahmen und detaillierterer Ausgestaltung des Datenschutzes gegeben. Zu erwähnen sind hier z.B. Regelungen betreffend Sicherheitsbehörden, Journalisten zur Wahrung des Redaktionsgeheimnisses sowie für künstlerische und literarische Zwecke zur freien Meinungsäußerung (Sokolov, 2018) und der informellen Selbstbestimmung betreffend des Allgemeinwohls für Kinder, die grundsätzlich

erst ab 16 in Datenverarbeitung einwilligen können. In Österreich sind bekanntlich unmündige Minderjährige unter 7 Jahren gänzlich geschäftsunfähig, bzw. bei anderen Minderjährigen beschränkt geschäftsfähig, d.h. geschäftsfähig nur mit Zustimmung deren gesetzlicher Vertreter (§21 und § 865 ABGB), ansonsten dürfen sie zwar Geschäfte zu ihrem Vorteil annehmen, jedoch nicht zu ihrem Nachteil. Ob hier eine Abschätzung der Folgen von Datenverarbeitungseinwilligungen gegeben ist, sei dahingestellt. Auch hier obliegt die Ausgestaltung der Regelungen betreffend Kinder den Mitgliedsstaaten (Art. 40 Abs. 2 lit. g). Insofern ist es auch nicht erstaunlich, die Verarbeitung von Kinderdaten in der EUDSGVO keiner Risikostufe zuzuordnen (Gierschmann et al., 2018, S.730). Zudem existieren Ausnahmen für wissenschaftliche und künstlerische, bzw. Archivierungszwecke (Gierschmann et al., 2018, S.526). Werden z.B. historische bedeutende Dokumente archiviert und finden sich darauf personenbezogene Daten, wäre es nicht praktikabel, die betreffenden Personen über die Datenverarbeitung zu informieren. Ähnlich verhält es sich mit Personen des öffentlichen Rechtes und Lebens wie Politiker, Schauspieler und Spitzensportler.

3.4 Datenschutzbeauftragte(r)

Eine mit Datenschutz beauftragte Person (Art. 37 EUDSGVO) ist dem Wort nach genau dafür zuständig: Datenschutz. Nach Art. 39 überwacht diese Person die Einhaltung des Datenschutzes wie z.B. hinsichtlich eingesetzter Software, der Mitarbeiter und generell des gesamten Unternehmens. Sie fungiert als Ansprechperson für Dritte außerhalb des Unternehmens und unterliegt der Geheimhaltungspflicht. Zu benennen ist eine derartige Person für ein Unternehmen sobald mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Da dies faktisch auf alle Webdesign-KMUs zutrifft, ist auch die Benennung erforderlich. Wichtig in diesem Zusammenhang ist, keine Person aus der Geschäftsleitung oder aus der eigenen IT-Abteilung zu benennen. Hier bestünde nämlich ein Interessenkonflikt, wonach sich die Kontrollierten selbst kontrollieren sollten (Solmecke et al., 2018, S.91) und genau dem will die EUSDGVO vorbeugen.

3.5 Datenschutzerklärungen

Solche sind auf Webseiten nach Inkrafttreten der EUDSGVO Standard. Diese müssen auf Datenverarbeitungen d.h. also Cookies und sonstige erhobene Daten auf der Webseite hinweisen, sowie deren Zweck (Art. 13 i.v.m. Art 6 EUDSGVO), also z.B. zur Vertragserfüllung für eine Bestellung. Einzige Ausnahme wäre eine rein private Seite im Rahmen familiärer oder persönlicher Tätigkeiten (Art 2. Abs. 2 lit. c EUDSGVO). U m nicht doch in Konflikt mit dem Datenschutz zu gelangen, sollten Log-Dateien beim Hoster deaktiviert sein und keine IP-Adressen länger als zur reinen Übertragung der Internet-Seite an das abrufende Endgerät gespeichert werden. Die EUDSGVO gilt letztlich ja nur für ganz oder teilweise automatisierte verarbeitete personenbezogene Daten oder Daten, die in Form eines Dateisystems organisiert sind (Art 2 Abs. 1 EUDSGVO). Sobald Daten erhoben werden, sei es durch Einbindung von Google Analytics, Kontakt-Formulare E-Mail-Adressen erfragen, Waren über einen Webshop verkauft werden, Cookies verwendet oder eine Webseite an Affiliate-Programmen teilnimmt, also kommerziell betrieben wird, sind Datenschutzerklärungen zwingend auf jeder Webseite erreichbar anzuzeigen. Diese richten sich nach Art und Umfang der erhobenen Daten, müssen in jedem Fall aber über den Zweck der Datenerhebung aufklären und die Kontaktpersonen nennen, an die man sich zwecks Wahrung der Auskunfts-, Änderungs- und Löschanträge wenden kann. Ferner muss bei Verwendung von Web-Shops über Datenweitergabe aufgeklärt werden. Zumindest Bezahldienstleister müssen zwangsläufig Daten des Kunden zwecks Rechnungsbegleichung übermittelt bekommen, also seine Kontodaten für Lastschriftverfahren oder die Kreditkartennummer. Erklärungen sind auf Webseiten jederzeit verfügbar zu halten und dürfen nicht in AGBs platziert werden (Solmecke et al., 2018, S.107). Die genannten Beispiele sind lediglich exemplarisch, weshalb auf die zu adaptierenden Mustererklärungen bei Solmecke et el. (2018, S.189ff.) verwiesen wird. Mustererklärungen speziell für Österreich finden sich z.B. bei der Wirtschaftskammer Österreich unter den weiter oben angeführten Links oder im abgespeicherten Zusatzmaterial zu dieser Arbeit – erhältlich unter www.Gosmann.at, bzw. auf CD, die der Druckversion dieser Arbeit an der FH-Burgenland beiliegt.

4 Arten von Daten – was darf man von Kunden überhaupt migrieren

Hinsichtlich neuer Haftungsfragen aus der EUDSGVO sind umfassende Aufklärungspflichten an Betroffene über Datenverarbeitung erforderlich. Das Problem wird deutlich, führt man sich vor Augen, wer Kunde eines Webdesign-Unternehmens sein kann. Die Palette reicht quer durch sämtliche Wirtschaftssektoren und alle Unternehmen mit unterschiedlichen Geschäftsfeldern. Da somit potentiell damit zu rechnen ist, es nicht immer mit IT-kundigen Personen hinsichtlich der einleitenden Problematiken zu IP-Adressen, Cookies, Log-Dateien sowie Speicherorten und Datentransfers zu tun zu haben, ist es logisch, Aufträge schlichtweg auf folgende Art zu erhalten: „Wir möchten eine Webseite. Darauf sollen folgende Informationen zu finden sein und folgende Produkte angeboten werden." Somit obliegt die Verantwortung für EUDSGVO-Konformität dem Webdesign-KMU.

4.1 Wartung und Betreuung: Webdesign-KMU oder Kunde?

Die erste grundsätzliche Frage die sich stellt ist, wer die Betreuung der Seite nach deren Erstellung übernimmt. Wird das Webdesign-KMU damit beauftragt oder nach Abnahme durch den Kunden selbst? Im ersten Fall verbleibt das Admin-Passwort zum jeweiligen CMS beim Webdesign-KMU, im zweiten wird dies dem Kunden ausgehändigt und geändert. Datenschutztechnisch geht es hier um die Verantwortung für den jeweiligen Content. Werden z.B. Bilder verwendet, die Datenschutzrechte verletzen, haftet derjenige, der die Seite betreibt. Wird diese Verantwortung an das Webdesign-KMU delegiert handelt es sich bei diesem um einen Auftragsverarbeiter für den Kunden mit entsprechender Haftung, denn die EUDSGVO sieht vor, sämtliche Beteiligte an einer Datenverarbeitung als Gesamtschuldner haften zu lassen (Art. 83 Abs. 3) - der Abschluss eines entsprechenden SLAs mit genauer Verantwortungsmatrix ist in diesem Fall unerlässlich, um nach der EUDSGVO nicht für Datenschutzverstöße durch Fehlbedienung der Webseite seitens des Kunden zu haften. Überträgt das Webdesign-KMU dagegen die volle Verantwortung für die Seite dem Kunden, so muss sichergestellt sein, eine Seite auszuliefern, die konform den neuen Regelungen der EUDSGVO ist. Anderenfalls gelten Haftungsregelungen in Zuge

klassischer Gewährleistung. Hier geht es darum, im Falle der Auslieferung von mit veralteten CMS erstellter Webseiten oder durch Zuhilfenahme veralteter Software, dem Kunden gegenüber ein fehlerhaftes Produkt zu liefern und dessen Daten ungewollt an die Hersteller der Software zu übertragen. Genau diese Angst, ungewollt Daten zu Cloud Providern zu übertragen und dadurch Konkurrenten oder Personen mit dubiosen Interessen zugänglich zu machen, stellt eine Hemmschwelle dar, deren Potential vollständig auszuschöpfen. Dagegen ist die Angst vor der EUDSGVO noch weniger stark ausgeprägt, zielt diese doch auch auf Großkonzerne und nicht auf KMUs. Sie sieht zwar Sanktionen vor, jedoch dienen die existenzbedrohende Strafen primär der Abschreckung von Großkonzernen wie Facebook, Google und Amazon.

4.1.1 Die verhängten Strafen

So hieß es mit Stand Februar 2019 seitens der offiziellen EU-Quelle in Form des Reportes des EU-Parlaments bezüglich der bisher seit 25.5.2018 verhängten Strafen nach der EUDSGVO, dass exakt 55.955.871 € an Geldbußen verhängt wurden (Hubert, 2019, S.13). Da davon 55 Mio. auf Google Frankreich entfielen, merkt man hier deutlich, dass die EUDSGVO tatsächlich auf massive Datenschutzverstöße von Großkonzernen abzielt und nicht kleine Unternehmen wie Webdesign-KMUs. Google verabsäumte es nämlich, Benutzer hinreichend über ihre Einwilligungsrechte zur Datenverarbeitung aufzuklären

Die Top-3 waren im Detail wie folgt:

- Den Spitzenplatz belegte mit 55 Mio. € Google Frankreich wegen besagter Informationspflichtverletzungen
- 400.000 € wurden gegen den „Zweitplatzierten“, ein portugiesisches Krankenhaus ausgesprochen, da Personal mit unzulässigen Accounts Patientendaten einsehen konnte und hier sensible medizinische Daten betroffen waren.
- 20.000 € für Platz drei wurden einem deutschen Blogger auferlegt, der Passwörter im Klartext speicherte.

Somit blieben 535.871 € und damit gerade etwas mehr als eine halbe Mio. €, die sich innerhalb der ganzen EU verteilten. Österreich war dabei mit einem Unternehmen vertreten, dass unzulässige Videoüberwachung durchführte und dafür 4.800 € auferlegt bekam (Porter, 2019).

4.1.2 Der österreichische Weg

Wenngleich Strafen wie oben angeführt gegen österreichische Unternehmen verhängt werden, bewegen sich diese in der Regel am unteren Limit. Auch von anhängigen Verfahren bei den österreichischen Höchstgerichten ist noch nicht viel zu bemerken. Die folgende Tabelle 3 zeigt, wie wenige Verfahren diesbezüglich mit Stand 5.5.2019 entschieden wurden.

Rechtsinformationssystem http://ris.bka.gv.at Datum: 5.5.2019 Rechtssätze und Entscheidungen								
Suchbegriff	**Oberster Gerichtshof**	**relevant davon**	**Verwaltungsgerichtshof**	**relevant**	**Verfassungsgerichtshof**	**relevant**	**gesamt**	**relevant**
Datenschutzbehörde	12	2	32	2	14	1	58	5
DSGVO	12	3	1	1	1	1	14	5
							72	**10**

Tab. 3: Verfahren zur EUDSGVO (eigene Darstellung, Daten aus https://ris.bka.gv.at)

Betreffend obiger Erkenntnisse sind grundsätzlich nur diejenigen nach dem 25.5.2018 relevant. Und von diesen waren einige noch mit „Auswertung in Arbeit“, bzw. betrafen nicht die Problematik mit Auswirkungen des Webdesigns. Diejenigen Erkenntnisse, die greifbar waren, finden sich in den abgespeicherten Quellen zu dieser Arbeit. Erkenntnisse der Datenschutzbehörde selbst sind dagegen nicht relevant, da deren Erkenntnisse nicht die letzte Instanz sind - deswegen lag an dieser Stelle der Fokus auf den Höchstgerichten.

Der Kunde muss sich jedenfalls darauf verlassen können, eine in Auftrag gegebene Webseite am Stand der Technik (Art. 32 EUDSGVO) zu erhalten. Was genau unter diesem Stand der Technik zu verstehen ist, ist strittig und mit Pseudonymisierung sowie Verschlüsselung knapp benannt, wie Gierschmann ausführt. Auch was Lizenzkosten anbelangt, ist erst abzuklären ob eine Lösung nicht mit Standardsoftware erzielt werden kann (2018, S.851). Auch Datenschutzaktivist Maximilian Schrems findet vieles in der EUDSGVO schwammig formuliert und bezeichnet es als „technisch schlechtes Gesetz“ (nach ORF Online 2, 2019). Gerade die SSL-Verschlüsselung zu implementieren ist

daher Pflicht für ein Webdesign-KMU. Was Standardsoftware zur Erstellung von Verarbeitungsverzeichnissen anbelangt, kann dagegen Excel als Standardlösung gute Dienste leisten, vorbehaltlich der Telemetriedaten, wie im entsprechenden Kapitel gezeigt wurde. Mit Libre Office finden sich aber auch Open Source Produkte im Angebot.

Kurioserweise sind die Regelungen zumindest für Österreich relativ zahnlos. Wie Müller treffend feststellt, fehlen weitgehend administrative Regelungen zur Zuständigkeit der Verhängung von Geldbußen. So normiert Art. 83 Abs. 9 EUDSGVO die Datenschutzbehörde des jeweiligen Mitgliedsstaates als die Instanz, die die Strafen verhängen kann, sollten sonstige nationale Regelungen für Geldbußen nicht vorgesehen sein (Müller, 2018, S.188). Geldbußen sind in Form von Verwaltungsstrafen in Österreich zwar sehr wohl vorgesehen, nicht aber das sofortige Abstrafen von Unternehmen bei Datenschutzverstößen. Für Österreich wird die Datenschutzbehörde dabei vom Bundeskanzleramt koordiniert und auch in technischer Hinsicht betreut (Datenschutzbehörde Österreich, 2018). Die Datenschutzbehörde soll jedoch primär verwarnen statt strafen und da Datenschutzverstöße in Österreich Verwaltungstatbestände sind, darf auch nicht mehr gestraft werden, wenn eine derartige Behörde bereits gegen ein Unternehmen eine Strafe verhängt hat. Damit werden die hohen Strafen der EUDSGVO faktisch umgangen (ORF Online, 2018). Dabei entgegen kommt der Republik Österreich sogar die EUDSGVO selbst. Es müssen nämlich auch andere Bußgeld-Bestimmungen für Verstöße gegen die Verordnung in nationalem Recht vorgesehen werden (Art. 84 EUDSGVO). Da somit die EUDSGVO nicht für jeden Verstoß von sich aus Geldbußen vorsieht, bleibt es daher den Mitgliedsstaaten selbst überlassen, wie hoch sie die Bußgelder, also Verwaltungsstrafen ansetzen.

Noch komplizierter wird es, wenn sowohl das Webdesign-KMU als auch der Kunde - und dies ist normalerweise die Regel – die Seite betreuen. Immerhin ist es dem Webdesign-KMU nicht zumutbar, jeden kleinen Änderungswusch, wie Text- oder Preisänderungen des Kunden vorherzusehen, andererseits ist es IT-unkundigen Kunden nicht zumutbar, technische Änderungen in Eigenregie durchzuführen. Auf den Punkt gebracht bedeutet dies: der Content stammt und

wird betreut vom Kunden. Die Technik und Implementierung betreut das Webdesign-KMU. Daraus ergeben sich eine Reihe von Problemen durch die EUDSGVO, wenn Daten durch fehlerhafte Implementierung unzulässig übertragen werden, allerdings auch wenn Content, der Datenschutzbestimmungen verletzt durch den Kunden eingepflegt wird. Um hier feststellen zu können, wer was wann eingepflegt hat und dem daher die Verantwortung zuzuweisen ist, sind einmal mehr Logfiles erforderlich. Wie bereits darauf hingewiesen wurde, muss man der Datenverarbeitung jedoch zustimmen. Es müssen daher wechselseitige Einverständniserklärungen des Webdesign-KMUs wie des Kunden vorliegen, hier die Daten des jeweiligen anderen zu verarbeiten. Problematisch erscheint in diesem Zusammenhang der Betrachter der Webseite, also der Endkunde. Denn dessen Daten, werden dann beiden Unternehmen zugänglich. Ob dies dem Sparsamkeitsgebot genügt darf bezweifelt werden. Daher müssen Datenschutzeinverständniserklärungen stets so gehalten werden, allen zum technischen Betrieb erforderlichen Speicherungen und Datenübertragungen aktiv durch Setzen von z.B. einem Häkchen zuzustimmen. (Erwägungsgrund 32 EUDSGVO)

4.2 Anforderungen betreffend des Contents

Was nun genau mit dem eigentlichen Content gemeint ist, hängt vom Auftraggeber und dessen Anforderungen ab. Werden also Webshops angeboten, ein Blog geführt oder lediglich eine bessere Visitenkarte der Firma ins Internet gestellt. Soll allenfalls ein Newsletter-System angeboten werden, bzw. erfolgt die Einbindung sozialer Netzwerke wie Facebook, Twitter, etc… und v.a. werden Kundendaten für Bestellungen oder zum Zwecke der Erstellung von Foren-, bzw. Blogbeiträgen gespeichert. Vom Umfang und der Wichtigkeit eines 24/7-Betriebees abhängig ist auch, welche Hoster letztlich gewählt werden und wie hoch dessen Verfügbarkeitsgrad ist. Eine Verfügbarkeit von 99,5% pro Jahr z.B. lässt sich einfach auf etwa 44 Stunden Ausfall pro Jahr umrechnen. Treten diese Ausfallzeiten werktags von 8-16h auf verliert man mehr als eine ganze Woche Produktivzeit. Die wohl wichtigste Frage ist aber, in welchem Rechenzentrum die Speicherung erfolgt. Je nach Art der Daten dürfen bestimmte

Daten nicht in Drittstaaten übertragen werden, was allerdings genau denn der Fall wäre, wenn Redundanz erforderlich ist und Rechenzentren außerhalb der EU als Backup fungieren. Wie Haselmann treffend feststellt, sind es bekannte Probleme jeglicher outgesourcten Beziehung, sich in ein Abhängigkeitsverhältnis zu begeben, sowohl was Infrastruktur, Kosten und eben auch Standorte betrifft (2012, S.91ff.). Als Webdesign-KMU kann man nicht wissen, ob der Kunde nicht eines Tages seine in Auftrag gegebene Webseite eigenmächtig zu einem anderen Hoster umzieht. Im Normalfall ist dies kein besonders schwieriges Unterfangen, da es im Kern darauf hinausläuft sämtliche Datenbanken eines CMS zu sichern, die gleiche Version am Ziel wieder zu installieren und die Datenbanken wieder einzuspielen. In Zeiten vor dem Aufkommen von CMS war dies sogar noch einfacher, da man lediglich den Inhalt des Webverzeichnisses 1:1 kopieren und die Berechtigungen am Ziel entsprechend setzen musste.

Zur Beantwortung der Frage, was denn nun von einem Kunden migriert werden darf, soll und auch muss, sei auf die erwähnten sechs Prinzipien verwiesen. Neben klassischen Impressumspflichten aus medienrechtlichen Bestimmungen der jeweiligen Mitgliedsstaaten. Für Webseiten bedeutet dies, die Datenschutzerklärungen immer abrufbereit zu halten und je nach Art des Unternehmens Besucher der Webseite umfassend aufzuklären, welche Daten zu welchem Zweck verarbeitet werden, wie lange diese gespeichert und an wen warum weiter transferiert werden sowie diese auf ihre Widerspruchs- (Art. 21 EUDSGVO), Richtigstellungs- (Art. 16 EUDSGVO) und Löschrechte (Art. 17 EUDSGVO) hinzuweisen.

Ansonsten muss sich das Webdesign-KMU auch auf die Aussagen des Auftraggebers verlassen und diesem vertrauen können, nur autorisiertes Datenmaterial zu erhalten in dem Sinne, die Webseite vom grundsätzlichen Design her gestalten zu können. Damit ist gemeint Firmenlogos, Fotos, Kontakt-E-Mail-Adressen, Namen von Mitarbeitern, etc…, d.h. also diese einer Veröffentlichung zugestimmt haben, möglicherweise sogar einer Veröffentlichung mit Bild. Betreffend Fotos wird noch auf die damit verbundenen Schwierigkeiten im weiteren Verlauf eingegangen. Allein

betreffend Namen von Mitarbeitern ist bereits fraglich dem Datenminimierungsgebot der EUDSGVO zu entsprechen. In den seltensten Fällen wird auf Webseiten tatsächlich der Name eines Mitarbeiters erforderlich sein. Anhand von E-Mail-Adressen, die in der Form vorname.nachnahme@unternehmen.at gestaltet sind, lassen sich jedoch schon Rückschlüsse ziehen, wer dahinter steckt. Bessere E-Mail-Adressen sind daher neutralisiert in folgender Form z.B. sekretariat@unternehmen.at oder sales@unternehmen.at zu verwenden. Auch hier muss man als Webdesign-KMU darauf achten, Kunden allenfalls auf diesen Umstand hinzuweisen. Sog. besondere Kategorien an Daten, also solche aus denen die Rasse, ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie genetische oder biometrischen Daten und Gesundheitsdaten oder zum Sexualleben sind generell untersagt, außer die betroffene Person stimmt dem ausdrücklich zu oder die Verarbeitung ist lebensnotwendig. (Art. 9 EUDSGVO). Einer Person jedoch zu erklären, die Verarbeitung der Information z.B. zur Blutgruppe falle unter das Sparsamkeitsgebot bei der Erhebung für einen Online-Einkauf, dürfte dabei interessant werden. Es ist somit davon auszugehen, auch hier nicht Daten willkürlich erheben zu dürfen, selbst wenn man im Vorfeld darüber aufklärt und beliebig viele Datenfelder in einem Formular vorzusehen, die nichts mit dem eigentlichen Ziel einer Webseite zu tun haben.

5 Der Grafikbereich und Cloud Services

In diesem Kapitel wird die Auswirkung der EUDSGVO auf die grafische Gestaltung einer Webseite betrachtet. Für das hier betrachtete KMU stellt sich die Frage, welche Quellen dafür verwendet werden. Steuert die Grafiken der Kunde bei, muss sich das KMU dennoch rückversichern, alle Rechte an grafischem Material eingeräumt zu erhalten, was die Verarbeitung zwecks Veröffentlichung im Rahmen des Auftrages auf einer Webseite beinhaltet. Werden hier Versäumnisse festgestellt, kann das KMU reagieren und die Verarbeitung ablehnen. Zulässig sind laut Datenschutz-Anpassungsgesetz 2018 Bildaufnahmen u.a. dann, wenn die Person zugestimmt hat, es in ihrem lebenswichtigen Interesse liegt oder es gesetzlich erlaubt ist – z.B. als Gruppe, wo die Person selbst nicht identifizierbar ist. Unzulässig ist es jedenfalls dann, wenn keine Zustimmung vorliegt oder der höchstpersönliche Lebensbereich verletzt wird, es der Überwachung am Arbeitsplatz dient oder eben die Daten mit anderen Daten zusammengeführt werden, worunter die Bilderkennung fällt (§ 11 und § 12 Datenschutz-Anpassungsgesetz 2018), wie derzeit massiv in China praktiziert.

Schwieriger wird die Verarbeitung, wenn das KMU mit der laufenden Wartung einer Webpräsenz beauftragt wird, wie im letzten Kapitel angesprochen, der Auftraggeber jedoch selbst administrative oder zumindest Autorenzugänge im CMS erhält. Damit kann dieser jederzeit selbst weitere grafische Elemente beisteuern. Diese Grafiken entziehen sich der Kontrolle des KMUs, was gleichbedeutend ist, bei Verstößen gegen die EUSDGVO im Rahmen der Mithaftung ebenfalls zur Verantwortung gezogen werden zu können, was die gemeinsame Betreuung der Webseite betrifft, außer man loggt die Zugriffe mit und weiß, wer für was verantwortlich war. Dies benötigt, wie angeführt wurde, ebenfalls die Zustimmung aller betroffenen Parteien, also dem Webdesign-KMU, dem Auftraggeber und der Endkunden.

Mögliche Verstöße bei Grafiken bestehen grundsätzlich in der Unterscheidung zwischen Fotos und echten Grafiken. Bei Fotos ist die Entscheidung oft schwierig, da v.a. bei sämtlichen abgebildeten Personen deren Einverständnis

zur Veröffentlichung vorliegen muss. Nun wird der Auftraggeber in den seltensten Fällen dem KMU entsprechende Einverständniserklärungen vorlegen können, geschweige denn, dem KMU auch zuzumuten, sich selbst die Personalausweise jeder Person vorweisen zu lassen. Eine Möglichkeit wäre daher die ausschließliche Wartungsübernahme einer Webpräsenz durch das KMU ohne Adminzugang für den Auftraggeber zu übernehmen oder die Ablehnung des Auftrages, um dabei keinen Verstoß gegen die EUDSGVO zu riskieren. Die andere Möglichkeit wäre die Verpixelung und damit die Anonymisierung abgebildeter Personen sowie identifizierbarer Daten wie z.B. KFZ-Kennzeichen oder Straßennamen und Hausnummern, bzw. militärischer Einrichtungen - hier liegt es am Auftraggeber, mit seiner Webseite nur grafische Elemente zu verwenden, die EUDSGVO-konform sind, bzw. zumindest entsprechend aufbereitet wurden.

Deutlich wird daher, bei Fotos, da es sich ja um urheberrechtliches Material handelt immer Gefahr zu laufen, Rechte Dritter zu verletzen. Für Videoclips auf Webseiten gilt im Wesentlichen das gleiche, da es auch hier um Lichtbildmaterial geht, dessen einziger Unterschied in der Bewegung besteht, bzw. bei Tonaufnahmen natürlich auch bei den Stimmen, bzw. der Musik. Anzumerken wäre, auch ohne EUDSGVO bei Verstößen betreffend Fotos zu haften, nicht jedoch nach datenschutzrechtlichen Bestimmungen, sondern nach urheberrechtlichen Bestimmungen mit Rechten an informeller Selbstbestimmung und damit verbundenen Rechten am eigenen Bild (§ 12 Datenschutz-Anpassungsgesetz 2018). Dieses ist ein Persönlichkeitsrecht und schützt die abgebildeten Personen nach urheberrechtlichen Bestimmungen vor unerlaubter Abbildung (Oesterreich.gv.at, 2019).

Andere Maßnahmen, die modernes Webdesign hinsichtlich grafischer Darstellungen für EUDSGVO-Konformität erfordert, sind die erwähnten soziale Netzwerke, allen voran Facebook und Twitter. War es vor der EUDSGVO Praxis, Content der sozialen Netzwerke mit entsprechendem HTML-Code in die eigene Webseite einzubinden, muss nun an dieser Stelle ein mehrstufiger Prozess implementiert werden. Dieser besteht darin, Nutzer darauf hinzuweisen, wenn

diese den Content tatsächlich anzeigen wollen, explizit zustimmen zu lassen, ihre Daten dem sozialen Netzwerk zur Verfügung zu stellen. Der Grund liegt in der automatischen Übertragung von Daten bereits zum Zeitpunkt des Aufrufens von Webcontent. Zu diesem Zeitpunkt käme jegliche Frage nach einem Einverständnis bereits zu spät. Problematisch daran sind die gesammelten Daten durch die sozialen Netzwerke. Da wäre zum einen die IP-Adresse, die ja – wie bei den Grundlagen erläutert wurde - technisch bedingt notwendig ist, um überhaupt Daten vom die Webseite hostenden Server abzurufen. Diese IP-Adresse allein liefert schon viele Informationen über die Nutzer, nämlich welcher Provider diese zur Verfügung stellt und aus welcher Region der Erde, konkret aus welchem Land die Seite abgerufen wurde. Dazu kommen noch Daten über den sog. User-Agent, d.h. also den Webbrowser, dessen Bildschirmauflösung, das verwendete Betriebssystem und allenfalls die ebenfalls erwähnten Cookies, sofern schon vom Besuch anderer Webseiten durch das soziale Netzwerk welche gesetzt wurden, um eine Wiedererkennung der Einzelperson herbeizuführen. Auch der sog. Facebook-Pixel ist an dieser Stelle erwähnenswert, der dazu dient Besucher zu tracken. Sog. EXIF-Informationen in Bildern tragen das Übrige zur Preisgabe von Informationen bei, können darin Meta-Daten hinsichtlich der Aufnahme wie Name der Person, GPS-Position, verwendetes Gerät, Seriennummer, etc… gespeichert werden.

Nachdem dieses Verhalten per se nicht EUDSGVO-konform ist, sind entweder die angeführten Informations-Maßnahmen fällig, bzw. muss das Webdesign-KMU Auftraggeber darauf hinweisen, auf Einbindung von Content aus sozialen Netzwerken zu verzichten. Die entsprechende Abwägung selbst obliegt dabei dem Auftraggeber. Die Mittel zur Verfügung zu stellen, um sich nicht strafbar zu machen muss dagegen das Webdesign-KMU in Form entsprechender Plugins, widrigenfalls hier eine fehlerhaft ausgelieferte und nicht dem Stand der Technik und den Anforderungen der EUDSGVO entsprechende Seite vorläge. Es gilt allerdings auch hier, die entsprechenden Scripts und Plugins, sofern einmal implementiert, als Referenz nehmen zu können. Die Kosten halten sich daher im Rahmen und können vernachlässigt werden, da jeder angestellte Programmierer

des Webdesign-KMUs nach technischer Anleitung aus dem Internet binnen weniger Minuten die Implementierung im Zuge seiner regulären Programmiertätigkeit vornehmen kann. Zusätzliches Personal dafür anzustellen ist somit nicht zwingend erforderlich.

6 Der Bereich Hosting

Was den Abruf einer Webseite anbelangt kann in Hinblick auf Unternehmen, deren Geschäftsbereich nicht im IT-Umfeld liegt, kaum verlangt werden über Detailwissen zu verfügen, welche technischen Prozesse im Hintergrund laufen, geschweige denn, wie Daten aus Webformularen verarbeitet werden. Das Zauberwort heißt hier Outsourcing und damit Abgabe von Verantwortung – eben an das Webdesign-KMU. Beim Webdesign handelt es dabei geradezu schon um eine normative Kraft des Faktischen. Webseiten werden über Endgeräte abgerufen, d.h. sie müssen zwecks Funktion gehostet werden und dieses „Gehostete" muss hergestellt, d.h. programmiert sein, um etwas Visuelles darzustellen, d.h. textuelle oder grafische Elemente – es muss anpassbar sein an verschiedene Endgeräte und daher über Responsive Design verfügen. Zudem muss es auf Datenschutz hinweisen.

6.1 Das KMU entwickelt, gehostet wird jedoch anderen Orts

Wie bereits auf die Problematik hingewiesen wurde, verfügt das hier betrachtete fiktive KMU zwar über Kenntnisse im Development und Erbringung von Serviceleistungen beim Webdesign, tritt jedoch nicht selbst als Hoster der so entwickelten Seiten auf. Zudem verfügt es nicht über eigene Testumgebungen und schon gar nicht über eigene IT-Infrastruktur, mit Ausnahme der Clients und einer redundanten NAS-Infrastruktur. Stattdessen wird auf das Pay-As-You-Go-Modell gesetzt, um sich de facto teure Server und die Kosten für deren Räumlichkeiten samt USVs, Löschanlage, Server-Monitoring, etc… zu ersparen und rein auf Services zu setzen (Abdoulaye, 2017, S.14). Details finden sich in den Tabellen und Erläuterungen zu den Auswirkungen der EUDSGVO auf das fiktive KMU. Was für die Hardware gilt, gilt auch betreffend aktueller Software. Sämtliche Arbeitsplätze damit auszustatten und Lizenzkosten zu bezahlen ist heute nicht mehr zeitgemäß. Stattdessen werden bei Bedarf entsprechende Produkte als Software as a Service gemietet, was im Zuge von sog. on Demand, bzw. Pay per Use-Modellen geschieht (Vossen, Haselmann, Hoeren, 2012, S.36f. u. 124f.). Auch Weinman erblickt in diesen Modellen einen gewissen Reiz, bezieht sich allerdings auf Rechenzentren, trifft jedoch die Problematik auf den

Punkt. Denn Software as a Service erfordert eine Infrastruktur und damit auch Rechenzentren, wo sie läuft. (2012, S.300). Somit müssen zwangsläufig Dienstleister damit beauftragt werden. Diese verarbeiten damit ebenfalls anfallende Daten des KMUs. Für den Auftraggeber ist jedoch erster Ansprechpartner bei Datenschutzverstößen nicht der Beauftragte des KMUs, sondern das KMU selbst - konsequenterweise haftet es auch dafür (Vossen et al., 2012, S.121).

Hosting ist somit der gefährlichste Bereich in Hinblick auf die EUDSGVO, etwas falsch zu machen. Hat man bis zur Veröffentlichung einer Webseite weitgehend die Kontrolle über Art und Umfang der potentiell anfallenden Daten, entzieht sich die Kontrolle darüber, wenn die Seite publiziert wird. Tritt das Webdesign-KMU selbst als Hoster auf, hätte es zwar die Kontrolle über die Server, nicht jedoch bei Übergabe an den Kunden, der das Hosting selbst einem anderen Anbieter überantwortet, was auch der Normalfall ist. So finden sich z.B. in den AGBs für ein typisch österreichisches Kleinstunternehmen, welches mit dem CMS-Wordpress arbeitet folgende Bestimmung: „eine gebrauchstaugliche Website auf Basis von WordPress herzustellen und diese auf dem Webspace des Kunden zur Verfügung zu stellen.“ (Retzl, 2019, S.2).

Der Auftraggeber lässt also eine Lösung vom Webdesign-KMU entwickeln, veranlasst dann jedoch deren Abrufbarkeit nach seinem Ermessen bei einem Cloud-Anbieter seiner Wahl im Zuge einer Storage as a Service-Lösung. Dies können auch die großen Anbieter Amazon Web Services, Microsofts Azure oder die Google Cloud sein (Weinman, 2012, S.91). Auch sich selbst einen Server im Zuge von Infrastruktur as a Service bei einem anderen Anbieter zu mieten käme in Frage. Dies wäre im einfachsten Fall der Internet-Provider, im andren Fall ein Rechenzentrum freier Wahl. In all diesen Fällen kann die Lösung des Webdesign-KMUs hinsichtlich Datenschutz noch so durchdacht sein, stimmen die SLAs des gewählten Rechenzentrums, bzw. Hosters nicht mit der aktuellen Rechtslage überein, hat der Kunde dann ein Problem, wenn es um Anfragen zur EUDSGVO oder gar um Nachweise der konformen Datenverarbeitung geht. Damit sind v.a. die vorhin genannten großen Anbieter gemeint, wenn

Rechenzentren außerhalb der EU zum Hosting verwendet werden. Leider ist dies immer dann der Fall, wenn redundante Anbindung gewünscht ist, was bei kommerziell genutzten Seiten durchaus logisch ist und somit andere Rechenzentren in anderen Erdteilen wie eben den USA oder dem asiatischen Raum als Backup fungieren. Eine Lösung wäre daher rein europäische Rechenzentren zu wählen.

6.2 Haftung und Verantwortlichkeit

Für den bekannten Like-Button, der als Facebook-Plugin eingebunden wird, haftet der Webseitenbetreiber für allfällige Datenschutzverstöße durch Facebook. Letztlich entscheidet ja der Webseiten-Betreiber über die Einbindung des Plugins (Gierschmann, 2018, S.93), das auf Datenverarbeitung hinweisen muss. Für die Auslagerung sonstiger Daten zu einem Cloud-Anbieter sind Betroffene ebenfalls im Vorfeld zu informieren, auch Cloud-Anbieter betreffend ihrer Rolle als Empfänger von Daten und als Auftragsverarbeiter für das beauftragende Unternehmen. Man darf sich hier allerdings auf sog. Kategorien von Empfängern beschränken und muss keine konkreten Personen benennen, was auch nicht praktikabel wäre bei einem Anbieter wie MS Azure oder Google und damit einer unüberschaubaren Art von Empfängern (Gierschmann, 2018, S.420).

In diesem Zusammenhang sei auch auf die Transparenz bei der Datenverarbeitung hingewiesen. Zwar ermöglicht die EUDSGVO die Wahrung eigener Interessen Betroffener. Diese Rechte jedoch in Anspruch zu nehmen wird allerdings auch auf diese abgewälzt. Ohne Anträge werden keinerlei Handlungsaktionen gesetzt. Bestand bisher wenig bis gar kein Interesse aus Angst vor dem bürokratischen Aufwand und wohl auch vor den Gerichtskosten, besteht kein Grund für die EUDSGVO Gegenteiliges anzunehmen, was einzelne Bürger und deren Rechtsdurchsetzung anbelangt:

„Mit dem Verweis auf eine effektive Wahrnehmung eigener Rechte wird die Verantwortung letztlich auf den Betroffenen verlagert. Dies ist bedenklich, weil die Fülle an Informationen und die große Komplexität der technischen Abläufe den Betroffenen regelmäßig überfordern dürfte,

soweit er überhaupt ein Interesse an den Informationen über die Datenverarbeitung hat." (Gierschmann et al., 2018, S.187)

Verarbeitungsverzeichnisse sind durch ein Webdesign-KMU jedenfalls zu führen, wenn Daten der Natur der Sache entsprechend regelmäßig verarbeitet werden (Art. 30 Abs. 5 EUDSGVO), bzw. auch besondere Kategorien von Daten, also „rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit [...], sowie [...] genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung" (Art. 9 Abs. 1 EUDSGVO). Beides ist im Normalfall beim Webdesign potentiell gegeben, da damit zu rechnen ist, es mit Kunden zu tun zu haben, deren Zielgruppe ein breit gefächertes Publikum für deren Webseiten ist und damit auch alle gesellschaftlichen Schichten diese Seite nutzen und auch potentiell ihre Daten verarbeiten lassen können.

Besonders hinsichtlich der Ersparnisse durch Verwendung keiner eigenen Hard- und Software sowie der damit entfallenden Wartungs- und Instandhaltungskosten ergeben sich mögliche Probleme hinsichtlich der EUDSGVO. Wurde bisher darauf abgezielt möglichst viele Services auszulagern und damit CAPEX-Kosten in OPEX zu wandeln (Weinman, 2012, S.98), die weitaus geringer sind, muss nun genau geprüft werden, wer welche Services anbietet und v.a. wo diese geographisch gesehen liegen.

Problematisch dabei ist für den Auftraggeber die Verantwortlichkeit, Cloud-Anbieter zu wählen, die entsprechende Garantien hinsichtlich EUDSGVO-konformer Datenverarbeitung bieten. Somit könnte sich ein Webdesign-KMU stets aus der Verantwortung stehlen. Dem ist jedoch nicht so, denn die hergestellten Cloud-Lösungen müssen ebenfalls konform sein (Obernosterer, 2017, S.57) – in diesem Fall eben die Software der Webpage. Ein anderes Problem stellt die sog. Schatten-IT dar. Angestellte des KMUs, die eigenständige Storage-Cloud-Lösungen verwenden, wie z.B. Onedrive oder Google Drive können so - wenngleich unbeabsichtigt - Daten von Kunden auf Servern außerhalb der EU speichern. Ob die Daten dort konform der EUDSGVO verarbeitet werden sei

dahingestellt. Der Kontrolle der IT des KMUs sowie der Kontrolle des Kunden sind sie jedenfalls entzogen (Obernosterer, 2017, S.44f.). Und wenn keiner der beiden um deren Speicherung weiß, wird auch keiner auf den Gedanken kommen, diese Daten zu löschen beantragen oder noch schlimmer, sollte der Kunde eine Auskunftsanfrage stellen, das KMU diese dahingehend sogar beantworten, keine Speicherung auf EU-fremden Servern vorzunehmen. Da dies trotzdem der Fall ist, drohen die Strafsanktionen der EUDSGVO spätestens dann, sollten daraus Daten verwendet werden. Immerhin sind die Betreiber von Public Cloud Services bekannt dafür, Daten entsprechend auszuwerten und zu nutzen. Dafür reicht eine E-Mail-Adresse, die der Kunde vielleicht ausschließlich dem Webdesign-KMU genannt hat. Sollte diese Adresse plötzlich anderweitig Verwendung finden, ist natürlich klar, wer die Schuld an der missbräuchlichen Verwendung trägt.

Da KMUs oft auch nicht über entsprechende Hardware verfügen, für ihre Auftraggeber „sicher" im Sinne der Schutzkriterien eines Rechenzentrums entsprechend die Daten zu speichern, greifen diese selbst auf Storage as Service-Lösungen zurück. Der Vorteil liegt auf der Hand: die Verantwortung für die Datensicherung obliegt dem jeweiligen Betreiber. Eigene kostspielige Hardware dafür ist ebenfalls nicht erforderlich und man kann sich auf die eigentliche Problemstellung konzentrieren, nämlich für den Kunden Lösungen zu entwerfen (Obernosterer, 2017, S.32f.). Der Nachteil: man weiß eben im Vorfeld nicht immer, welche Daten der Auftraggeber zu verarbeiten gedenkt. Selbst wenn ein Kunde mitteilt, er speichere bloß Kundenadressen, ist noch lange nicht gesagt, es hier in der Zukunft nicht doch mit Daten anderer Natur, wie z.B. medizinischen Daten zu tun zu haben. Einer Datenbank selbst ist es nämlich egal, welche Felder zusätzlich angelegt werden und welche Daten über ein erweiterbares Webformular abfragbar sind. Ein CMS ermöglicht es ja weitgehend selbst Erweiterungen vorzunehmen und ohne Wissen des ursprünglich implementierenden KMUs hier für entsprechenden Wildwuchs zu sorgen. Es sei an dieser Stelle einmal mehr auf die Problematik der Regelung von

Modifikationen verwiesen, wer also den Content und wer das technische Design der Seite ändert.

Am meisten genutzt werden seitens KMUs folgende Cloud-Services: E-Mail mit einem Anteil von 65% und Storage as a Service-Lösungen mit 62% (Obernosterer, 2017, S.17). Bedenklich erscheint dies insofern, als der E-Mail-Verkehr mit Kunden meist über Microsofts Exchange-Server abgewickelt wird, der ja laut Erhebungen in der Schweiz einen dortigen Marktanteil im Jahr 2016 von 64% hatte (IT-Markt, 2017, S.4). Wie bei neueren Microsoft-Produkten üblich und beim Kapitel zu der Überprüfung durch das niederländische Innenministerium gezeigt wurde, ist das „nach Hause telefonieren" dabei grundsätzlich eingebaut. Der Exchange-Client ist nun mal Outlook aus der Microsoft Office Suite und die Autodiscover-Funktion trägt beim Kontaktieren der Server das Übliche dazu bei.

Da faktisch alle Informationen heutzutage zwischen einem Webdesign-KMU und dem Kunden per E-Mail ausgetauscht werden, wird deutlich, welchen Stellenwert Datenschutz hier hat. Noch deutlicher wird dies bei der Speicherung. Ohne das Wissen in welchem Rechenzentrum Daten generell abgelegt werden, ist eine konforme Verarbeitung nach der EUDSGVO unmöglich. Problematisch dabei ist wiederum, vielfach außer Zusagen der Rechenzentrumsbetreiber kaum Möglichkeiten in der Hand zu haben, dies zu verifizieren. Selbst wenn eine Delegation des KMUs oder auch deren Auftraggeber sich in einem Rechenzentrum ankündigen und diesem dann einen Besuch abstatten, kann ohne technisches Detailwissen kaum die Einhaltung überprüft werden. Eine Möglichkeit diesem Umstand gegenzusteuern wären Zertifizierungen nach entsprechenden ISO-Normen. Hervorzuheben wäre z.B. die Eurocloud-Zertifizierung, die durch entsprechende Audit-Verfahren gewährleistet, dass die überprüften Rechenzentren die jeweiligen Standards einhalten. Dies geschieht in Form von festgelegten Kriterien-Katalogen. Damit wird es zwar deutlich schwieriger, Datenschutzverletzungen zu vertuschen, wenngleich 100% Sicherheit auch hier nicht existiert. V.a. was in der Zwischenzeit zwischen einem Audit und einer Rezertifizierung passiert, bleibt offen. Dennoch verpflichtet die EUDSGVO Unternehmen zur Setzung technischer und organisatorischer

Maßnahmen. Genau diese können interne und externe Audits auf deren Tauglichkeit hin überprüfen (Gierschmann, 2018, S.710). Betreffend Strafen und Haftungsfragen ist es jedenfalls schwieriger, diese gegen ein KMU oder dessen Kunden durchzusetzen, wenn dieses auf entsprechende Zertifizierungen verweist. Generell ist man darauf angewiesen, auf das zu vertrauen, was einem der SLA-Partner sagt. Somit muss man diesem vertrauen, wenn er behauptet, sich an ein SLA zu halten (Vossen et al., 2012, S.185). Zwingend vorgesehen sind dabei Auftragsverarbeitungsverträge in Schriftform oder mittels elektronisch signierter Dokumente. Hält sich ein Auftragsverarbeiter nachweislich nicht an die Bedingungen und Weisungen des Auftraggebers, haftet dieser selbst für Datenschutzverstöße (Solmecke et al., 2018, S.61ff.). In diesem Zusammenhang eröffnet sich ein Forschungsfeld für sog. Smart Contracts, da anzunehmen ist künftig eine Vielzahl ähnlicher Verträge mit einer Vielzahl an Auftragsverarbeiter abschließen zu müssen.

Letztlich hängt es auch von den Anforderungen der Kunden ab, in wieweit hier welche Cloud-Lösung zum Einsatz kommt. Reines Hosting von Webseiten, die lediglich PR-Zwecken dienen und außer dem Unternehmensgegenstand, der Firmenadresse und einer allfälligen Kontakt-E-Mail nichts weiter beinhalten, können hier ohne Weiteres zu einem Storage-Anbieter ausgelagert werden. Zu achten ist allerdings auf entsprechende SLAs, die dafür Sorge tragen, auf die Speicherung der IP-Adresse und allenfalls Cookies, wenn z.B. Werbeschaltungen in Kooperation mit Partnerunternehmen geschaltet werden, hinzuweisen.

Als Webdesign-KMU hat man nun das Dilemma, die Kunden auf genau diese Problematiken hinzuweisen. In den nächsten 4-5 Jahren findet der große Umbruch insofern statt als es keine lokal installierbaren Versionen kommerzieller Anwendungen wie in der heutigen Form mehr geben wird und man nicht mehr entscheiden kann, was man on-premises und was in der Cloud – egal welche Form – hostet. Angepeilt ist seitens Microsoft das Jahr 2023. Die Wahl existiert somit nicht mehr zwischen hybriden Cloudformen oder der Wahl anderer Lösungen - von IaaS über PaaS bis zu Software und Storage as a Service gleichermaßen. Diese „Schönheit“ der hybriden Cloud-Lösungen, die

sich noch bei Weinman finden (2012, S.164f.), wird daher auf absehbare Zeit nicht mehr existieren. Dies mag grundsätzlich nicht schlecht sein, immerhin erspart man sich von Administratoren über eigene Infrastruktur bis hin zu Stromkosten erheblich viel Geld, gleichzeitig riskiert man infolge der EUSDGVO hohe Strafen, wenn man sich nicht um SLAs kümmert, bzw. konkret die Wahl des Rechenzentrums. Denn auch hier liefert man als Webdesign-KMU nur das Produkt, nicht jedoch die Laufzeitumgebung, also die Hardware oder jeweilige Cloud-Lösung für das eigentliche Hosting.

6.3 Datensammlungsfreudigkeit der NSA und der Cloud Act

Bedenken müssen Kunden generell, sich beim Internet als weltweites Netzwerk in permanenter Geiselhaft der Netzwerkbetreiber zu befinden. Die beste on-premises-Lösung nutzt nichts, wenn die Webpage nicht erreichbar ist, da die Netzwerk-Infrastruktur nicht korrekt funktioniert. Dieses Problem betrifft häufig kleinere Internet-Provider ohne redundante Anbindungen zum Endkunden. Konkret wären daher auch hier Lösungen in Rechenzentren, die mehrfach redundant angebunden sind zielführender mit dem Risiko, EUDSGVO-konformen Mehraufwand zu tätigen, v.a. was die angesprochene Replikation und Redundanz betrifft. Außerhalb der EU gelten ja andere Datenschutzbestimmungen, wie z.B. in den USA. Den eigentlichen Anlassfall hierzu hat wohl im Jahr 2013 Microsoft geliefert, als es sich weigerte, E-Mail-Daten auf Servern in Irland den US-Behörden zur Verfügung zu stellen. Sollte auch nur ein US-Unternehmen in irgendeiner Form an Datenverarbeitung außerhalb den USA beteiligt sein, können die Geheimdienste dank des Cloud-Acts von Donald Trump sehr wohl auf sämtliche Daten zugreifen (Mewes, 2018). Der Cloud Act selbst basiert dabei auf dem Stored Communications Act, der schon 1986 Gesetz war (Swire Daskal, 2019).

Damit dürfen die USA faktisch auf sämtliche Daten weltweit zugreifen, denn US-Unternehmen sind fast überall am Betrieb von Rechenzentren beteiligt. Für Deutschland wurde jedoch ein Rechenzentrum, das Microsoft ursprünglich für seine Cloud-Services betrieben hatte, der deutschen Telekom überantwortet. Das Modell wurde deswegen aufgekündigt weil die Funktionen sehr eingeschränkt

waren und um technisch – mangels Zugriffsmöglichkeit – gar nicht mehr in der Lage zu sein, Daten-Anfragen zu beantworten. (Schüler, 2018). Denn offiziell dürfen die USA damit nicht mehr auf diese Daten zugreifen. Seit Edward Snowden weiß die Welt jedoch um die generelle Datensammlungswut der NSA Bescheid, Cloud Act hin oder her.

6.4 Lösung: Rechenzentren – besser als ihr Ruf

Allerdings bestehen entgegen der Annahme, wonach in Rechenzentren generell alles schlechter wäre, da man keine Kontrolle über die Daten hat, deutlich bessere Abwehrmöglichkeiten gegen Hacker und die NSA, anstatt wie bei vielen on-premises Lösungen. Die Rede ist hier nicht nur von der Wahl von EU-Produkten sowie entsprechender Antiviren-Lösungen, wie z.B. Firewalls, deren Hersteller nicht in den USA beheimatet sind, sondern auch vom Vertrauen auf die Experten des Rechenzentrums. Rechenzentren werden normalerweise im 24/7-Betrieb überwacht und ständig mit neuesten Patches und Updates versorgt. Wie Hugos und Hulitzky treffend anführen, obliegen Restores internen Administratoren, wobei die Qualität im Sinne von rascher Wiederherstellung und Reaktion von deren Fähigkeiten abhängt. Somit übersteigen Weiterbildungsmaßnahmen in neue Technologien und Personal schnell die Hosting-Kosten bei einem Cloud Service Provider, der eine Vielzahl an Mitarbeitern dafür beschäftigen muss, was schon alleine deshalb für ein KMU de facto nicht möglich ist. Spezialisten haben naturgemäß mehr Erfahrung, da sie ständig mit derartigen Szenarien konfrontiert sind, d.h. deren Fachwissen kann in dieser Hinsicht eine Verbesserung für den Kunden darstellen (Hugos, Hulitzky, 2011, S.93)

Als Webdesign-KMU müsste man hier dennoch Vorsorge tragen, eine Seite nicht replizierbar zu programmieren, will man dem Dilemma des Datenschutzes und der -sicherheit vorbeugen. Ziel könnte eine Art Geo-Blocking der Webseite selbst sein. „Stellt diese fest“ sie wird außerhalb der EU betrieben, so könnte sich die Webseite sperren. Ob dies bei tatsächlichem Ausfall eines Rechenzentrums die zielführende Intention ist, sei jedoch dahingestellt.

7 Der Bereich Development

Wesentlich beim gesamten Development-Prozess sind entsprechende Vereinbarungen mit Mitarbeitern, wonach dienstlich erstellte Scripts und erhobene Daten auf Speichern, bzw. Storage as a Service-Lösungen des KMUs abzulegen sind. Der Sinn dahinter ist, beim Ausscheiden einer Person aus dem Unternehmen auf Daten und von ihr geschaffene Werke ansonsten keinen Zugriff mehr zu haben. Damit wäre das Know how dieser Person für das Unternehmen verloren (Bundesministerium Digitalisierung und Wirtschaftsstandort, 2017, S.53). Erschwert wird dieser Umstand dadurch, Firewalls des Unternehmens in der Regel nicht so einfach dahingehend anpassen zu können, die namhaften Anbieter von Lösungen wie Microsoft Azure, Amazon Web Services oder Google Cloud einfach zu sperren. Dies wäre zwar technisch möglich, würde dann jedoch auch das Webdesign-KMU von der Erbringung von Dienstleistungen für die Kunden abhalten. Was Mitarbeiter dazu veranlasst, ihre Lösungen auf eigenen Storages abzulegen, liegt auf der Hand. Sollten Weblösungen entwickelt werden, die eine Adaptierung erfordern, was de facto alle sind, werden auch Scripts entsprechend adaptiert. Somit fehlt dem Webdesign-KMU der sog. generelle Source-Code, wenn Mitarbeiter diesen unter Verschluss halten. Bei in Webseiten implementierten Java-Programmen, die z.B. auf Tomcat-Servern laufen, reicht es ja aus, diese zu compilieren, ohne überhaupt den Quellcode zu veröffentlichen.

7.1 Daten von Auftraggebern auf Mitarbeiterspeichern

Datenschutzrechtlich noch problematischer wäre es, wenn Mitarbeiter auf ihren privaten Speicherbereichen Daten des Unternehmens oder vom Auftraggeber ablegen. Hier haftet für Verstöße grundsätzlich das Unternehmen (WKO 9, 2018), der Arbeitnehmer dagegen je nach Grad der Fahrlässigkeit. Bei leichter Fahrlässigkeit gar nicht, bei „normaler“ Fahrlässigkeit geteilt mit dem Unternehmen, bei grober Fahrlässigkeit tendieren Gerichte zwar bis zu drei Monatsgehältern, es kann jedoch auch höher sein, wobei bei es bei Vorsatz zu voller Haftung kommt (Datenschutzbeauftragter-info.de, 2018). Ob nun bewiesen werden kann, entsprechende Daten vorsätzlich auf eigene Speicher

ausgelagert zu haben, sei auch hier dahingestellt. Moderne Betriebssysteme wie Windows 10 haben die hauseigenen Storage-Lösung Microsoft Onedrive bereits fest implementiert und lagern, wenn man nicht aufpasst, automatisch Daten dorthin aus. Dies betrifft einmal mehr v.a. die Office Versionen, die bereits – wie erwähnt sehr datensammlungsfreudig sind, was vom niederländischen Innenministerium festgestellt wurde. Allerdings verfolgen auch andere Hersteller wie Adobe und Google entsprechende Interessen. Wird z.B. bei laufendem Google Backup and Sync-Client ein USB-Datenträger angeschlossen, was durchaus von einem Auftraggeber sein kann, der seine Daten darüber angeliefert hat, anstatt mehrere Gigabyte an Daten per Mail zu senden, erfolgt auch hier der automatische Upload, sofern ein unbedachter Klick zu viel erfolgt. Problematisch wird dies dann, wenn der Kunde sensible Daten anliefert, die erst im Zuge des Processings durch das Webdesign-KMU verarbeitet werden müssen, der Kunde jedoch keine Zustimmung zur Speicherung seiner Daten auf Drittservern - in diesem Fall denen von Goolge - erteilt hat. Mag es auch noch so viel Aufklärung im Vorfeld der Installation des Google Backup und Sync-Clients gegeben haben und das Webdesign-KMU diesem auch zugestimmt haben - der Auftraggeber tat dies nicht. Trotzdem finden sich seine Daten dann potentiell auf Servern bei Google USA.

7.2 Data Breach-Meldungen sind Pflicht

Damit wird einmal mehr deutlich, wie wichtig die Wahl von Rechenzentren ist, genaue Unternehmens-Policies zu definieren, welche Cloud-Anbieter genutzt werden dürfen und welche Services verboten sind (Bundesministerium Digitalisierung und Wirtschaftsstandort, 2017, S.53). Hält man sich nicht daran und würde o.a. Unfall passieren, wäre eine Data Breach Meldung an den Auftraggeber fällig. Ob dieser dann noch weiter Interesse an einer Zusammenarbeit mit dem Webdesign-KMU hat, sei dahingestellt. Hier merkt man besonders, welche Auswirkungen die EUDSGVO hat. Normalerweise würde ohne diese keine Meldung erfolgen und alles wäre ok, außer eben, beim Auftraggeber möglicherweise mit Spam-Mails rechnen zu müssen, wenn Google an seine Werbepartner entsprechende Informationen verkauft. Genau mögliche

Datenlecks bei Anbietern jeglicher PaaS-Lösung, auf denen andere Lösungen fußen, sind ein großes und leider auch unkalkulierbares Sicherheitsrisiko (Jamsa, 2013, S.38). Unkalkulierbar deshalb, da kein Anbieter von sich aus zugeben wird, er verstößt gegen Datenschutzbestimmungen, was sich nicht notwendigerweise auf die EUDSGVO beziehen muss. Datenschutzgesetze gibt es nämlich auf dem gesamten Globus verteilt, wobei deren individuelles Schutzniveau und Detailausgestaltung von Nation zu Nation variiert. Eine gute Übersicht findet sich z.B. bei Soares, Gallmann und Basil (2017, S.6ff.). Genereller Tenor dabei ist, es hier viel mit Vertrauen zu tun zu haben. V.a. in den USA wo hinsichtlich Datenschutzes die gegenteilige Meinung vertreten wird, nicht die Daten der Nutzer zu schützen, sondern die Daten bei den Unternehmen, ist man nach dem erfolgreichen Zu-Fall-Bringens von Safe Harbor durch Maximilian Schrems auf den Nachfolger Privacy Shield angewiesen (Solmecke et al., 2018, S.67). Dieser soll garantieren, Daten, die in die USA übertragen werden, auf gleichem Schutzniveau wie in der EU zu verarbeiten. Kontrollieren lässt sich dies freilich nicht, allenfalls lediglich durch die bereits angesprochenen Zertifizierungen im Zuge von Audits durch unabhängige Prüfer. Eurocloud z.B. zertifiziert hier weltweit nach den in der EU geltenden Standards. Andere Möglichkeiten sich auf ein entsprechendes Schutzniveau zu verlassen sind sog. Angemessenheitsbeschlüsse der EU-Kommision (Art. 44 EUDSGVO). Inkludiert mit dem Inkrafttreten der EUDSGVO waren die folgenden Staaten (WKO 8, 2019):

- Andorra
- Argentinien
- Färöer Inseln
- Guernsey
- Insel Man
- Israel
- Jersey
- Kanada
- Neuseeland

- Schweiz
- Uruguay
- USA (Privacy Shield vorausgesetzt)

und seit dem ersten separaten Beschluss seit der EUDSGO vom 23.1.2019

- Japan

Um es deutlich zu sagen: alle anderen Drittstaaten bieten kein ausreichendes Sicherheitsniveau für Datenverarbeitungen. Datenübertragungen ohne Zustimmung Betroffener dorthin gelten als Data Breach. Eine Standortwahl von Rechenzentren dort verstößt ebenfalls gegen die EUDSGVO, sollten Daten dorthin transferiert werden und keine Zertifizierungen dieser Zentren selbst vorliegen.

Verfügt jedoch ein Anbieter über Zertifizierungen, kann man sich als Webdesign-KMU „im Vertrauen darauf" berufen und haftet folglich nicht, wenn der jeweilige Auftragsverarbeiter Datenschutzverstöße begeht, denn mehr als sich davon zu überzeugen, dieser halte Datenschutz-Bestimmungen ein, kann man als reines Webdesign-KMU nicht tun. Ein Besuch der Rechenzentren vor Ort durch das eigene Personal des Webdesign-KMUs wird im Normalfall an der räumlichen Distanz - Rechenzentren können überall in der EU sein - als auch am fehlenden Know how, physische Server betreiben zu können, scheitern. Webdesign ist ja nach wie vor Softwareentwicklung und Anwendung. Das Webdesign-KMU mag somit Webseiten entwickeln können und auch über Erfahrung im softwaremäßigen Hosting-Bereich verfügen. Ob es auch über Wissen um Cluster-Lösungen für 24/7-Betrieb, redundante Anbindung ans Internet, bzw. Spanning-Tree-Protokoll (Krishnan, Bhagwat, Utpat, 2014, S.1f.) für zentrale Core-Switches, Wiederherstellung in Form von schneller Time to Recovery, etc… verfügt, darf bezweifelt werden. Würde das KMU über diese Erfahrung verfügen, könnte es ja selbst Anbieter entsprechender Lösungen sein.

7.3 Sicheres Löschen von Daten

Unter der EUDSGVO droht jedenfalls dann der Auftragsverlust, wenn Data Breach-Meldungen unterlassen werden. So drohen die einleitend erwähnten hohen Strafsanktionen, doch angesichts des Umstandes, einmal eingegebene Daten nur schwer wieder löschen zu können, erscheinen 4% vom Jahresumsatz oder 20. Mio. Euro durchaus gerechtfertigt (Art. 33 EUDSGVO). Es muss daher bereits bei der Webentwicklung dafür Sorge getragen werden, Daten nachweislich und sicher löschen zu können. Hunzinger weist in einem ganzen Buch treffend auf die Problematiken des „Löschens in Datenschutzrecht" hin. Viel zu einfach lassen sich in heutiger Zeit Kopien von Daten anfertigen. Zu Recht weist er auf den Rechts- und Kontrollverlust im digitalen Zeitalter hin. Sämtliche Datenschutzbestimmungen aller Staaten zielten ja letztlich mit Löschverpflichtungen auf die physische Vernichtung des jeweiligen Papieraktes ab (Hunzinger, 2018, S.216f.). Daten, die im Cloud-Zeitalter in einem Rechenzentrum liegen, lassen sich jedoch nicht durch Zerstörung mittels Sprengung selbigen vernichten. Dies ist durch redundante Auslegung von Rechenzentren vielfach auch gar nicht möglich. Daten zu Löschen bedeutet daher sie lediglich als gelöscht zu kennzeichnen, um sie vor weiterer Verwendung auszuschließen. Physisch sind sie jedoch immer noch vorhanden. Erst, wenn sie überschrieben wurden, d.h. derjenige physische Speicherplatz auf Festplatte, Band, USB-Stick,... tatsächlich andere Daten erhalten hat, sind die Daten gelöscht. Allerdings muss auch hier sofort wieder relativiert werden: eben nur dort. Andere Datenträger, wie Backups oder auf andere Standorte ausgelagerte, redundante Speicherorte sind davon nicht erfasst und müssten gesondert berücksichtigt werden. Die EUDSGO trägt diesem Umstand insofern Rechnung, als auf die Einhaltung eines angemessenen Schutzniveaus unter Berücksichtigung der Implementierungskosten abgestimmt wird (Art. 32 EUDSGVO), während man grundsätzlich dazu gehalten ist, für entsprechende Sicherheit der Verarbeitung zu sorgen, was besagte Backups einschließt, im Sinne eines unbeabsichtigten Verlustes (Art. 5 Abs. 1 lit. f EUDSGVO). Konkret bedeutet dies, für Backups zwar sorgen zu müssen, im Falle einer Löschaufforderung, jedoch nicht allen Datenträgern nachzujagen und dort die

Daten zu löschen, sondern durch geeignete Verfahren sicherzustellen, dass gelöschte Daten nicht wieder Verwendung finden, auch im Falle eines Restores.

Für das Webdesign-KMU bedeutet dies, genaue Arbeitsverzeichnisse zu führen, wo welche Daten gespeichert sind und im Falle eines Löschansuchens tatsächlich alle Daten von den operativen Datenträgern zu überschreiben. Leider ist auch dies oftmals nicht praktikabel, da dies zu erheblichem Aufwand führen würde und bei Datenbanken noch Datensätze durch Primary Keys davon mit sog. kaskadierter Löschweitergabe davon abhängig sein könnten. Die EUDSGVO begnügt sich daher auch hier mit dem Stand der Technik und der Wirtschaftlichkeit. Löschen dem Stand der Technik nach durch Überschreiben sollte dabei nach Regierungsrichtlinien in Form von mehreren Überschreibvorgängen erfolgen (BSI 1, 2018, S.171ff.). Viele Standard-Antiviren-Lösungen bieten sog. Shredder-Optionen, wie auch Open Source und Freeware-Tools. Wirtschaftlich dagegen ist es nicht sinnvoll, auch die Backups zu löschen. Man wäre allerdings gut beraten, im Optimalfall Primary-Keys zu setzen und zu vermerken, dass die in einem Backup zugeordnete Datensätze gelöscht wurden. Sollte nämlich ein Backup wiederhergestellt werden, wo die Daten noch vorhanden sind und ein Newsletter-Versand, trotz Zusicherung an Betroffene die Daten wären gelöscht, erfolgen, so hätten dies sofort eine Beschwerdemöglichkeit. Dazu reicht eine einfach Excel-Datei mit den Keys und dem Lösch-Vermerk. Damit sind die Daten erstens pseudonymisiert, da aus dem operativen Datenbestand schon gelöscht und daher nicht mehr abfragbar, im Falle eines Restores jedoch müssen diese Daten nachträglich nochmals gelöscht werden. Alles Gesagte gilt natürlich nur, sofern keine gesetzlichen Aufbewahrungsfristen bestehen wie steuerrechtliche Verpflichtungen.

7.4 Sonderfall: SSDs

Daten auf magnetischen Speichern lassen sich einfach löschen, indem sie überschrieben werden. Dies gilt jedoch nicht für SSDs. Die Speicherzellen darin haben nämlich eine begrenzte Lebensdauer, weshalb die Kontroller-Logik Schreibvorgänge auf den gesamten Datenträger verteilt. Ein Überschreib-Kommando ginge folglich ins Leere, da nicht sicher ist, die eigentlichen Daten

auch zu löschen. Spezial-Tools können derartige Datenträger Sektor für Sektor auslesen und auch so zu den eigentlich gelöscht geglaubten Daten kommen. Im Normalfall werden diese zwar fragmentiert sein, da dies schon zum Zeitpunkt der Speicherung so geschehen ist, dennoch reicht es für Textdateien aus, einzelne Fragmente zu erhalten, um sie wieder zusammensetzen zu können. Greift man auf gängige Sektoren-Größen mit 512 Bytes bis 64 KBs zurück, so lässt sich daraus schon sehr viel Information auslesen. Für das Webdesign-KMU wäre daher anzuraten, entweder nur magnetische Datenträger zu verwenden oder aber im Falle der Verwendung von SSDs, diese einem kompletten Durchlauf zu unterziehen, wenn Daten gelöscht werden sollten. Auf diese Weise ist sichergestellt, die gesamte SSD zu löschen.

7.5 Kernaufgaben des Develpments

Im Kern lassen bei der Umsetzung der EUDSGVO für das Development folgende Aufgaben definieren (Solmecke et al., 2018, S.27):

- sämtliche Datenverarbeitungsvorgänge im Unternehmen identifizieren
- prüfen, ob diese der EUDSGVO entsprechen, was vielfach nicht oder nicht gehörig der Fall sein wird
- Erstellung einer Liste sämtlicher Auftragsverarbeiter, d.h. besonders hierunter fallen Hoster und Cloud-Lösungsanbieter
- prüfen, ob ein Datenschutzbeauftragter zu benennen ist
- prüfen, ob bei der Erhebung der Daten, sämtliche Informations- und Transparenzpflichten gegenüber den Betroffenen eingehalten werden
- Prozesse implementieren, die den Rechten auf Auskunft, Widerruf, bzw. Änderung und Löschung Betroffener gerecht werden
- Entwicklung eines Konzeptes, die gespeicherten Daten zu schützen - dies betrifft insbesondere Integrität, Authentizität, Vertraulichkeit und Verfügbarkeit - hat man nämlich Daten nicht verfügbar im Sinne diese bei Bedarf auszuheben, kann man auch keinerlei allfälligen Auskunftsbegehren nachkommen
- schriftliche Prüfungen, ob eine Datenschutz-Folgeabschätzung zu erstellen ist
- Durchführung regelmäßiger Schulungen beim Personal

Da dabei letztlich immer das Development hinsichtlich der Implementierungen betroffen ist, können obige Punkte nur in Zusammenarbeit mit den Developern

geschehen. Wer sonst sollte wissen, welche Daten tatsächlich von einer Webseite erhoben werden oder ein Konzept ausarbeiten, diese Daten zu schützen?

Künftig sind Webseiten dahingehend zu entwickeln sog. Privacy by Design zu bieten, also von Grund auf datenschutzfreundlich programmiert zu werden, andererseits sind Endgeräte und Software auch durch Privacy by Default so einzustellen, entsprechende Schutzeistellungen vorkonfiguriert zu bieten (Solmecke et al., 2018, S.53f.), also out of the box. Für die Geräte nutzenden Personen bedeutet dies im Gegensatz zu früher, nicht aktiv nach Datenschutzeinstellungen suchen zu müssen - jeder der ein Android Smartphone in der Hand hatte, weiß, wie mühsam dies sein kann und auch wie schnell man dort oder da eine Einstellung übersieht. Es müssen daher erst aktiv Einstellungen gewählt werden, Daten preisgeben zu wollen. In Zusammenhang mit dem erwähnten Kopplungsverbot ergeben sich auch hier interessante Konstellationen und Betätigungsfelder für Gerichte. Immerhin ist die Nutzung des Google Playstores ohne einen Google-Account und damit eine E-Mail-Adresse nicht möglich. Ohne den Playstore jedoch erhält man auf regulärem Wege keine Updates für Apps und ohne Updates öffnet man bekanntlich entdeckten Sicherheitslücken Tür und Tor, die v.a. darauf abzielen, Daten abzugreifen und zu missbrauchen. Dieser Umstand betriff auch Webdesign-KMUs, da Webseiten auch auf mobilen Endgeräten angezeigt werden. Somit müssen zwangsläufig Seiten auch auf entsprechenden APPs und Developer-KITs getestet werden. Damit ist einmal mehr die Problematik verbunden, Gefahr zu laufen, Kundendaten an Google zu übertragen.

Auswirkungen existieren auch beim geplanten Vertuschen von Datenpannen. Wurden früher Datenschutzverstöße möglichst geheim gehalten, um keine Negativ-PR zu bekommen, sieht die EUDSGVO vor, binnen 72 Stunden nach Bekanntwerden die Datenschutzaufsichtsbehörde zu informieren, es sei denn ein Risiko für persönliche Rechte Betroffener und Freiheitsrechte stünden dem entgegen (Solmecke et al., 2018, S.76). Beispiel: das Passwort einer Auftraggeberin, die Dienste als Prostituierte auf einer Webseite anbieten möchte wird vorzeitig gehackt. Eine Meldung an die Datenschutzbehörde würde

angesichts der gemeinhin als verwerflich angesehenen Dienste in diesem Fall die Kundin in ihrem Recht auf Privatsphäre verletzten und damit an ihren persönlichen Rechten. Denn auch die Datenschutzbehörde muss nicht den Realnamen der Kundin mitgeteilt bekommen, zumal diese dann letztlich bei der Datenschutzbehörde verächtlich gemacht werden würde.

8 Der Bereich Datenbank

Zentraler Regelungsbereich der EUDSGVO sind geradezu Daten. Wie der Name schon sagt, werden diese Daten entweder in einer Art Verzeichnisstruktur oder eben in Datenbanken gespeichert. Was das Webdesign-KMU intern betrifft, ist an dieser Stelle gemeint, es mit den Kundendatenbanken sowie Webdatenbanken im Hintergrund von CMS als sog. Backend-Service zu tun zu haben.

8.1 Die Datenübertragbarkeit

Hinsichtlich des o.a. Developments stellen sich dabei auch neue Herausforderungen hinsichtlich der Datenübertragbarkeit (Art. 20 EUDSGVO). Betroffene haben nämlich durch die EUDSGVO das Recht erhalten, ihre bekannt gegeben Daten zu einem anderen Anbieter zu übertragen (Solmecke et al., 2018, S.79). Für das fiktive Webdesign-KMU heißt dies, v.a. beim Development und Datenbanken darauf zu achten, standardisierte Exportformate zu unterstützen, die auch eingelesen werden können. Wird eine Webseite entwickelt, ist daher dafür zu sorgen, es dem Kunden zu ermöglichen, die Daten auch abgreifen zu können. Zu denken wäre an entsprechende Interfaces, da nicht alle Personen mit der Kommandozeile zum Erstellen von sog. SQL-Dumps umgehen können. Genau solche Dumps von Datensätzen allerdings müssen angefertigt werden, sollen sie standardisiert wieder eingelesen werden, da es sich um reine Textdateien handelt. Die Schaffung von Interfaces oder Gewährung des Shell-Zugang zwecks SQL-Dump-Anfertigung bedeutet jedoch wieder ein Sicherheitsrisiko mehr.

In diesem Fall könnte die Webseite selbst in Form von Storage as a Service bei einem Anbieter gehostet, die Datenbank dagegen in Form von Software as a Service wo anders betrieben werden. Welcher Art diese Datenbank ist, bleibt dann dem Auftraggeber vorbehalten. Im Klaren muss sich dieser jedoch sein, es mit Cloud-Strategien großer Anbieter wie MS SQL-Server oder Oracle zu tun zu haben, die neuerdings ihre Unternehmensstrategie darauf ausgerichtet haben, ihre Dienste nur mehr als Software as a Service-Cloud-Lösung anzubieten. Der Vorteil: als Kunde hat man immer die dem aktuellen Stand der Technik

entsprechende Version mit allen Updates, der Nachteil: ohne Kunde dieser Anbieter zu werden, bleibt man bei on-premises-Lösungen mit neu entdeckten Sicherheitslücken dem Risiko ausgesetzt, nicht am Stand der Technik nach der EUDSGVO compliant zu sein. Umgekehrt steckt man im Dilemma, Daten möglicherweise in die USA oder andere Drittstaaten zu transferieren, ohne dies zu wissen, sollte man bei der Wahl des Rechenzentrums nicht aufgepasst haben und möglicherweise den Auftraggeber auch gar nicht darüber informiert. Was das Webdesign-KMU anbelangt müssten ja zumindest ansatzweise auch Daten vorliegen zwecks Test der Webseite. Oft ist es auch unerlässlich mit Echtdaten zu testen, wenn reale Einsatzbedingungen überprüft werden sollen.

8.2 Einwilligung in die Verarbeitung als Pflicht

Rechtssicher ist es bei Datenbanken immer, wenn die Einwilligung Betroffener zur Verarbeitung erfolgt oder gesetzliche Erlaubnistatbestände vorliegen, d.h. sog. Verbot mit Erlaubnisvorbehalt. Konkret müssen Betroffene im Vorfeld über den Verarbeitungsvorgang und den Zweck der Erhebung der Daten informiert werden, um sich nicht auf überraschende Datensammlung berufen zu können. Dies schmälert dabei nicht deren Abänderungs-, Widerspruchs- und Löschrechte. Problematisch an diesen Einwilligungen erscheint jedoch selbst deren Rechtssicherheit. Ohne gültige Unterschrift oder digitale Signatur, sind Einwilligungen selbst digitale Daten, die gefälscht sein könnten, Stichwort: Identitätsdiebstahl. Zu den Problematiken hinsichtlich der Einwilligung finden sich viele Beispiele bei Solmecke et al. (2018, S.46ff.) – auch alle Formen des Hackings- und dem Ausnutzen von Sicherheitslücken durch Exploits gehören dazu. Darüber findet sich Literatur in Hülle und Fülle. Da hier jedoch niemand dazu angestiftet werden soll, zum Hacker zu werden, unterbleiben entsprechende Literaturhinweise. Stattdessen soll auf entsprechende Möglichkeiten der Absicherung von Systemen, das sog. Härten hingewiesen werden. Informationen dazu finden sich sehr wohl im erwähnten IT-Sicherheitshandbuch der Wirtschaftskammer sowohl für KMUs wie Mitarbeiter als auch in den Grundschutzkatalogen des Bundesamtes für Informationssicherheit in Deutschland. Wesentlich an dieser Stelle ist, als

Verantwortlicher alles mit vertretbarem wirtschaftlichen und technischen Aufwand Mögliche zu tun, um Exploits zu verhindern. Lässt man z.B. eine SQL-Server-Datenbank ungeschützt mit dem „sa“-User oder verwendet nur ein schwaches Root-Passwort für MySQL- / Maria-Datenbanken oder für das zugrunde liegende Betribessystem selbst ein schwaches Admin- oder Root-Passwort, grenzt dies an Fahrlässigkeit. Darunter fallen Passwörter wie „123456“ oder bekannte Begriffe wie der Name des Haustieres oder das Geburtsdatum. Das Unterlassen aktueller Virenscans oder dem Verwenden von in modernen Betriebssystemen implementierten Firewall-Systemen fällt ebenfalls in diese Kategorie. Beide Produkte sind mittlerweile kostenlos im weit verbreiteten Windows 10 erhältlich, wobei relativiert werden muss, wie festgestellt wurde, es defaultmäßig mit einem datenschutzrechtlich sehr auskunftsfreudigen Betriebssystem zu tun zu haben.

Besonders im Datenbank-Bereich ist man gehalten, ständig Sicherheitsupdates einzuspielen, was hostenden Systeme betrifft. Ist ein Server nur mangelhaft geschützt und fallen einem Angreifer Zugangsdaten dafür in die Hände ist es nämlich ein Leichtes einen Dump sämtlicher Datenbanken zu ziehen. Es wäre dann nicht der erste Bericht über gehackte E-Mail-Zugänge und entwendete Kreditkarteninformationen aus dem Internet.

An dieser Stelle muss man als Unternehmen bedenken, sich auch um Backup as a Service-Lösungen bei anderen Anbietern zu kümmern. Sollte die Datenbank verloren gehen, stehen Fragen, wie Time to Recovery oder Grad der Wiederherstellbarkeit im Raum. Kommt 24/7-Betrieb ins Spiel, ist die Frage nach dem redundanten Standort relevant –also innerhalb oder außerhalb der EU. Damit einhergehend ist die Frage nach der Zulässigkeit der Übertragbarkeit oder des Backup dorthin generell verknüpft. Als Webdesign-KMU hat man hier erhebliche Sorgfaltspflichten als Auftragsverarbeiter für einen Auftraggeber zu bedenken, d.h. v.a. über die möglichen Risiken aufzuklären und entsprechend EUDSGVO-feste Lösungen anzubieten für die man auch hinreichende Garantien bieten muss (Art. 28 EUDSGVO).

8.3 Prinzipien und Verpflichtungen im Detail

Was Daten in Datenbanken anbelangt gelten zusammengefasst direkt aus der EUDSGVO übernommen die bereits bei Gobeo erwähnten folgende Prinzipien:

- *Grundsatz der Zweckmäßigkeit* (Art. 5 Abs. 1 lit. b EUDSGVO)
  Es dürfen Daten nur zum vorgesehenen Zweck erhoben, nicht auch anderweitig verwertet werden ohne Zustimmung.

- *Grundsatz der Datenminimierung* (Art. 5. Abs. 1 lit. c EUDSGVO)
  Hier dürfen nur erforderliche Daten abgefragt werden, um die Leistung auch zu erbringen. Für vorhin genannten Newsletter ist dies somit lediglich die E-Mail-Adresse erforderlich.

- *Grundsatz der Datenrichtigkeit* (Art. 5 Abs. 1. lit. d EUDSGVO)
  Betroffenen wird das Recht eingeräumt, Fehler in ihren Daten beseitigen zu lassen. Verarbeiter dagegen sind verpflichtet, diesem Wunsch nachzukommen und auf dem aktuellen Stand zu halten.

- *Grundsatz der Speicherbegrenzung* (Art.5 Abs.1. lit. e EUDSGVO)
  Daten dürfen nur solange gespeichert werden, wie für die Erbringung eines Vertragsverhältnisses erforderlich. Nach Erbringung einer Lieferung bei einem Online-Einkauf z.B. sind die Daten nach Ablauf der jeweiligen steuerrechtlichen Aufbewahrungsfristen zu löschen.

- *Grundsatz der Integrität und Vertraulichkeit* (Art. 5. Abs. 1 lit. f EUDSGVO)
  Hier geht es um den Schutz der Daten beim Transport, was in der Regel Verschlüsselungspflicht bedeutet, genauso wie Sicherung der Infrastruktur im Unternehmen vor willkürlicher Zerstörung und Änderung. Konkret sind damit Zugangskontrollen und Rechtevergabe nur an dazu befugte Personen gemeint, also das mindestens erforderliche Recht um eine Aufgabe auch durchzuführen. So braucht die Buchhaltung Zugriff auf Kundedatenbanken zwecks Rechnungslegung. Der Grafiker dagegen braucht Zugriff auf übersandtes Bildmaterial des Kunden, wogegen diesen Zugriff die Buchhaltung wiederum nicht braucht, usw... Problematisch erscheint in diesem Zusammenhang die Allmächtigkeit von Systemadministratoren.

- *Rechenschaftspflicht* (Art. 5 Abs. 2 EUDSGVO)

  Dies betrifft Auskunftsrechte und Protokollierungspflichten der Datenverarbeitung, also auch Log-Dateien.

Auch das schon erwähnte Verarbeitungsverzeichnis ist hinsichtlich Datenbanken für das fiktive KMU Pflicht. Zwar müssen solche Verzeichnisse eigentlich erst Großunternehmen ab 250 Beschäftigten führen, die EUDSGVO erlegt diese Verpflichtung allerdings auch KMUs dann auf, wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt besondere Datenkategorien, bzw. Daten über strafrechtliche Verurteilungen erfolgen (Art. 30 EUDSGVO). Da nur eine einzige dieser Gegebenheiten ausreicht und ein Webdesign-KMU der Natur der Sache nach permanent Daten verarbeitet, ist somit ein Verarbeitungsverzeichnis zu führen. Inhalt hat dabei zu sein woher, zu welchem Zweck sie verarbeitet werden, wer Zugriff hat und wohin sie weitergegeben werden. Ebenfalls werden ein Verantwortlicher benötigt, wie Solmecke treffend feststellt (Solmecke et al., 2018, S.70f.).

9 Allgemeine CAPEX / OPEX

Betreffend Kosten ist in diesem Kapitel festzuhalten, lediglich bei der Implementierung von Prozessen und für die Erfüllung von Dokumentationspflichten Investitionen, die sich auf sowohl auf die CAPEX- wie OPEX-Kosten niederschlagen, tätigen zu müssen.

Die Rede ist primär von einer Software zur Verwaltung von Verarbeitungsprozessen und entsprechender Musterdokumente. Wie einleitend erwähnt, ließe sich dies auch gänzlich ohne Spezialsoftware erledigen, da Word und Excel grundsätzlich ausreichend wären. Dennoch ist eine solche Herangehensweise nicht zu empfehlen. Erstens kann mit Spezialsoftware nachgewiesen werden, sich der EUDSGO ernsthaft angenommen zu haben und zweitens halten sich die Kosten dieser Spezialsoftware mit rund 300 € in Grenzen, wie z.B. für OTRIS Privacy, wobei das Mitmodell in etwa auf 1.600 € käme mit Stand Mai 2019. Für das Webdesign-KMU ist jedoch ein einzelner PC dafür vollkommen ausreichend, da das Definieren der Prozesse lediglich eine einmalige Aufgabe ist, die dann nur mehr adaptiert wird, wenn sich die EUDSGVO etabliert hat. Damit wäre die Spezialsoftware für die EUDSGVO abgedeckt. Zudem bietet das eigentliche Outsourcing laut der Auswirkungstabelle einer mit Datenschutz beauftragten Person, die schon über entsprechende Software verfügt, ebenso wie die Miete anderer Spezialsoftware als Software as a Service hinreichende Lösungsmöglichkeiten. Die Details hierzu sind den abgespeicherten Inhaltsanalyse-Quellen und den Ergebnis-Tabellen zu entnehmen.

Den Zugriff auf die EUDSGVO selbst gibt es im Internet in Form von PDF-Dateien ebenfalls der dieser Arbeit beigefügten Quellen oder unter dem URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679.
Es blieben daher noch die Fragen nach dem Personal offen, um die Verarbeitungsprozesse zu definieren und Verfahren einzupflegen, konkret also wer dies macht. Diesbezüglich ist anzumerken, die Verfahren das bestehende Personal im Zuge eines Brainstormings niederschreiben zu lassen und dieses dann von der mit Datenschutz beauftragten Person prüfen und entsprechend

ableitbare Prozesse gegenchecken zu lassen. Der Aufwand beim hier betrachteten KMU hält sich somit mit den Personal- und Kundendatenbanken in Grenzen, denn alles andere wird vom Auftraggeber bestellt und nach dessen Erfordernissen entwickelt.

Sollte eine zusätzliche Person dafür angestellt werden, schlägt sich dies allgemein in den OPEX-Kosten für das Personal nieder. Empfehlenswert ist jedoch, aus dem bestehenden Personal – trotz Outsourcings - eine weitere mit Datenschutz beauftragte Person zu benennen (Art. 37 EUDSGVO). In diesem Fall wirkt sich dies positiv auf die Personalintensität aus, da bestehende Ressourcen besser genutzt werden. Doch selbst im Falle des Anstellens einer zusätzlichen Arbeitskraft wirkt sich exklusiv arbeitendes Personal für Datenschutz positiv auf die Reputation des Unternehmens aus. Es kann daher an dieser Stelle nicht gesagt werden, die EUDSGVO verlangt übermäßigen Aufwand bei der Dokumentation der Prozesse und Datenverarbeitungen, zumindest für ein KMU der hier betrachteten Größe von zwölf Personen. Wie dies bei Großkonzernen und –unternehmen aussieht kann dagegen nur vermutet werden, nämlich mit erheblichen Mehraufwand rechnen zu müssen, besonders dann, wenn es um Unternehmen in Wirtschaftssektoren geht, die im Kerngeschäft nichts mit IT zu tun haben, sondern lediglich viele Daten verarbeiten wie Finanzdienstleister, Versicherungen oder große Handelsketten. Dies böte noch Stoff für weitere Forschungsfragen in diese Richtung.

Betreffend technischer Maßnahmen, sei auf die SSL-Verschlüsselung verwiesen, die nur eine einmalige Implementierung kostet, was das bestehende Development-Personal leisten kann. Das eigentliche SSL-Zertifikat ist entweder kostenlos zu beziehen – auch hier sei auf die Auswirkungstabelle verweisen, wenn es im Hosting-Paket inkludiert ist, oder es fällt nur ein geringfügiger Betrag an, wenn man sich Zertifikate von einer Zertifizierungsstelle wie z.B. Godaddy ausstellen lässt.

Die für das KMU anfallenden Kosten bei der Umsetzung der EUDSGVO sind somit leicht wettzumachen, führt man sich vor Augen, besonders hinsichtlich der

Cookie-Hinweise sowie der geplanten ePrivacy-Verordnung mit vielen Aufträgen an Webdesigner rechnen zu können – 10% sind es in der CAPEX / OPEX-Tabelle im Anhang basierend auf den Daten der Inhaltsanalyse. Eine Handvoll entwickelter Webseiten deckt somit bereits die Kosten vollumfänglich ab.

10 Ergebnis, Schlussfolgerung und Diskussion

Betreffend Auswirkungen der EUDSGVO auf ein fiktives Webdesign-KMU existiert eine Vielzahl programmierten Webseiten mit Cookies, die v.a. bei Online-Warenkörben davon abhängig sind, sei es durch die erwähnten Session- Cookies oder permanenter Art. V.a. deswegen muss man seitens der Betreiber dahingehend tätig werden, EUDSGVO konform zu werden und die Seiten umrüsten lassen. Es bleibt abzuwarten, wie hier Lösungen aussehen werden, v.a., wenn künftige Webbrowser von Vornherein so eingestellt sein müssen, kein Tracking zuzulassen, also keine Cookies zu setzen. Nur weil dies bisher nicht der Fall ist, ist die Default-Einstellung Cookies anzunehmen als keine generelle Einwilligung Betroffener zu deren Verwendung anzusehen (Solmecke et al., 2018, S.147).

10.1 Umrüstungen von Webseiten bringen Geld

Angesichts der daher zu erwartenden Umrüstungen durch Auftraggeber hinsichtlich Aufklärungspflichten im Vorfeld, bzw. generell der Sicherstellung der erwähnten Grundprinzipien erscheinen die eigenen Maßnahmen für das fiktive Webdesing-KMU bei der Umsetzung hinsichtlich Verarbeitungsverzeichnisse und der Benennung von mit Datenschutz beauftragten Personen marginal, weshalb dies Kosten daher zu vernachlässigen sind. Die Verpflichtung EUDSGVO-konform zu werden trifft, wie einleitend erwähnt, alle Wirtschaftssektoren, den konkreten Vorteil aus dem mehr oder weniger erzwungenen Development für fast drei Viertel aller Unternehmen ziehen letztlich jedoch Webdesign-KMUs. Andere Wirtschaftssektoren haben – es müsste weitere Forschung zeigen, ob es zutrifft – naturgemäß mit Mehrkosten zu rechnen. Handwerksdienste und Industrieunternehmen z.B., die Kundendaten speichern und international vernetzt sind, d.h. Daten zu Aufträgen und Lieferanten weltweit speichern, haben mit deutlichen Mehrkosten zu rechnen. Diese Unternehmen lukrieren selbst nichts aus der EUDSGVO, müssen aber trotzdem ihre Bestimmungen einhalten, um nicht mit den einleitend erwähnten Strafen belegt zu werden.

Die konkreten Auswirkungen auf das fiktive Webdesign-KMU finden sich in der Tabelle im Anhang. Im Rahmen der EUDSGVO stiegen kurzfristig die Entwicklungskosten für KMUs generell. Diese Kosten konnten jedoch aus marktwirtschaftlichen, bzw. strategischen Gründen nicht an den Endkunden weitergegeben werden. Stattdessen sind diese Kosten als zukunftsträchtige Investition anzusehen, über einen Wettbewerbsvorteil gegenüber nicht der europäischen Union angehörenden Unternehmen zu verfügen. Hervorzuheben wären v.a. Privacy by Design, das weltweit in Software implementiert wird, mit der Webseiten abgerufen werden. Damit sind Browser, aber auch Clients des Internet of Things gemeint, die z.B. Webservices nutzen. Auch hier ist dem Datensammlungsinteresse der Betreiber durch die EUDSGVO Rechnung zu tragen. Da sowohl Webservices wie auch klassische Internet-Angebote dem Internet-Charakter entsprechend weltweit abrufbar sind, sind Interessenten eher dazu geneigt, diese dort abzurufen, wo ihre Privatsphäre standardmäßig gewahrt wird. Derzeit ist das die europäische Union da es weltweit kein vergleichbares stärkeres Schutzrecht für Einzelpersonen vor unverhältnismäßiger und unzweckmäßiger Datenverarbeitung gibt, wenn die Verarbeitung nicht für die Leistungserbringung erforderlich ist.

10.2 Auswirkungen in Drittstaaten und Haftungsfragen

Konkret bedeutet dies, mit der EUDSGVO Wirkungen auch über die EU hinaus auf andere Anbieter zu erzielen. Diese Anbieter aus Drittstaaten, sofern es sich um gefestigte Demokratien handelt, haben naturgemäß ebenfalls Interesse daran, Auftraggeber weiterhin mit durchdachten Webdesigns zu versorgen. Die Auftraggeber dagegen wollen nicht nur auf Drittstaaten beschränkt sein, ihre Webseiten anzubieten, sondern v.a. in der wirtschaftlich starken EU. Demzufolge müssen auch von Unternehmen in Drittstaaten entwickelte Webseiten EUDSGVO-konform sein. Auf den Punkt gebracht kann es sich somit kaum jemand leisten, Geld für Webdesign auszugeben, welches aus einem weltweit umspannenden Netzwerk nicht im EU-Raum abrufbar sein darf. So war z.B. die Seite der L.A.-Time lange Zeit nicht aus Europa erreichbar.

Durch die Omnipräsenz von Datenschutzverletzungen moderner Hard- und Software kommt KMUs im Bereich Webdesign zwecks Haftung nur eine untergeordnete Rolle zu, da die Gesellschaft offenbar schon derart abgestumpft ist, trotz EUDSGVO die Verstöße zu tolerieren oder schlichtweg durch die hohe Anzahl zu resignieren. Hinzu kommt eine allgemein träge Justiz und hohe Kosten bei der Rechtsdurchsetzung, da vielfach bei höheren Streitwerten ohne Anwälte kein Verfahren eingeleitet werden kann. Insofern ist zu folgern, mit der EUDSGVO zwar grundsätzlich Mittel in die Hand zu bekommen, gegen Datenschutzverstöße vorzugehen, de facto werden Verstöße in Österreich erst abgemahnt und dann erst bestraft, was auch dann nur geschieht, wenn schwerwiegende Verstöße vorliegen. Für KMUs im Bereich Webdesign wäre es geradezu eine Kunst, sich aufgrund der EUDSGVO strafbar zu machen. Wie in dieser Arbeit gezeigt wurde, gibt es erstens kaum Handlungsbedarf hinsichtlich des Personals und zweitens, dort wo Handlungsbedarf besteht, nämlich im Design von Webseiten selbst kann man sich bei Open Source Lösungen und Freeware von CMS bedienen, was auch nur einmalig zu geschehen hat wie bei den erwähnten Cookies, aber auch bei der mehrstufigen Zustimmung zur Einbindung von Webcontent sozialer Netzwerke. Umgekehrt wirkt sich die EUDSGVO als PR- und Marketing-Instrument positiv auf ein KMU aus, kann es doch immerhin damit punkten, für sog. Privacy Sorge zu tragen.

Ungeklärt bleiben dagegen Fragen hinsichtlich Webdesigns für Minderjährige. Da hier die Öffnungsklauseln beschränkt sind, nicht unter 13 Jahren wirksam in Datenverarbeitung einwilligen zu können (Müller, 2018, S.189), bleibt fraglich, wie diese Zielgruppe überhaupt moderne Smartphones und Tablets nutzen soll. Da diese ja geschäftsunfähig ist, könnte sie nicht rechtsgültig Cookie-Hinweisen auf Webseiten zustimmen und in allfällige Datenschutzerklärungen einwilligen. Die Datensammlung erfolgt allerdings durch die Software trotzdem. Was generell die Frage nach der Haftung durch Verletzung der EUDSGVO anbelangt, sind richtungsweisende Entscheidungen der Höchstgerichte zum Zeitpunkt dieser Arbeit noch ausständig.

Kreditkarten- oder Ausweisdaten über das Internet zur Alters-Verifikation zu schicken, wäre jedenfalls wieder eine Datenverarbeitung. Hier läge ein interessanter Forschungsansatz für weitere Arbeiten in diesem Bereich vor. Andere Ansätze ergeben sich im Schadenersatzrecht. Da die EUDSGVO noch recht junge Materie ist, sind auch entsprechende Höchstgerichtsentscheidungen noch dünn gesät, bzw. zu einzelnen Bereichen ausständig. Ob tatsächlich Unternehmen durch existenzbedrohende Strafen am Weiterexistieren gehindert werden, muss angesichts des damit einhergehenden Job-Verlustes für die Angestellten und der damit einhergehenden steuerlichen Einnahmequellen für den Staat sowie allfälliger nicht mehr hergestellter Produkte oder erbrachter Dienstleistungen auch noch erforscht werden.

10.3 Beantwortung der Forschungsfragen

Hier wurde ein KMU für Webdesign betrachtet. Für dieses kann als Ergebnis die zentrale Forschungsfrage nach EUDSGVO-Konformität bei gleichzeitiger Beibehaltung der Senkung der Kosten für die IT durch Cloud-Lösungen dahingehend beantwortet werden, lediglich mit marginalen Auswirkungen auf das operative Tagesgeschäft zu rechnen. Wie einleitend erwähnt wurde, bieten sich sogar Vorteile gegenüber Mitbewerbern außerhalb der EU. Privacy by Default und Privacy by Design werden besonders mit der ePrivacy-Verordnung zu weiteren Verschärfungen im Datenschutz und zu Folgeaufträgen an Webdesigner führen. Es bleibt ein weites Betätigungsfeld, was auch die Nutzung von maßgeschneiderten Cloud-Umgebungen jeglicher Art, also IaaS, PaaS, SaaS, bzw. hybride Lösungen und Virtualisierung generell angeht, um Hardware besser auszunutzen, deren Administration zu vereinfachen und im Falle des Absturzes einer – virtuellen - Maschine nicht alle anderen laufenden Prozesse auf anderen Maschinen mit abstürzen zu lassen (Vossen et al., 2012, S.17f.). Für das Webdesign-KMU heißt dies, auf einem virtuellen Server-Systeme für verschiedene Kunden verschiedene Implementierungen gefahrlos testen zu können – sog. Responsive Design für verschiedene Endgeräte.

Betreffend der Unterfrage, was alles gespeichert und verarbeitet werden darf, lautet die Antwort schlichtweg: alles, dem zugestimmt wurde, jedoch

standardmäßig erst einmal gar nichts, es sei denn gesetzliche Pflichten bestehen hierzu, d.h. das sog. Verbot mit Erlaubnisvorbehalt. Sensible und kritische Daten, die in der Arbeit erwähnt wurden dürfen generell nicht verarbeitet werden, es sei denn es ist lebenswichtig, oder es wurde auch hier ausdrücklich zugestimmt und man sammelt diese Daten nicht bloß um deren Selbstzweck, sondern zu konkreten Zwecken.

Entgegen der Erwartungshaltung hinsichtlich der zweiten Unterfrage, es mit einer Verteuerung der Leistungen im Bereich des Webdesigns- und -programmierung zu tun zu haben, konnte festgestellt werden, lediglich kurzfristig mit marginalen Anschaffungen in diesem Bereich rechnen zu müssen. Tatsächlich handelt es sich um einmalige Investitionen, die, wie die einleitenden 30% Personen anführten, tatsächlich zu Vorteilen im Sinne eines Auftragsplus führten – hier waren es 10% zusätzliches Volumen. Da das Internet ein weltumspannendes Netzwerk ist und die EU mit ihren rund 512 Mio. Einwohnern als westlich orientierter Absatzmarkt für chinesische und amerikanische Unternehmen gilt, sind diese sehr wohl darauf bedacht, sich an die EUDSGVO zu halten. D.h. auch, in diesem Bereich - v.a. den USA - mit freiberuflichen Programmierern zu rechnen, die ihre Tools als Open Source und Freeware veröffentlichen, welche dann auch von europäischen Unternehmen genutzt werden können. Die Kosten für Eigenentwicklungen in diesem Bereich halten sich somit auch in diesem Bereich in Grenzen und können faktisch mit Null angesetzt werden. Deutlich wurde dies bei gängigen Content Management Systemen wie Joomla, Typo 3 oder Wordpress auf denen eine Vielzahl an kommerziellen Webseiten zwar basiert, die Systeme jedoch frei verfügbar sind und Erweiterungen in Form von Plugins zur Darstellung für Cookie-Hinweise, deren Einstellungen und Belehrungen über Datenschutz, bzw. -verarbeitung sich dabei ebenfalls kostenlos downloaden lassen.

Geklärt werden muss jedoch im Zuge weiterer Forschung die Frage nach bestehenden Cloud-Lösungen Großbritanniens, denn der „Brexit“ wird - unabhängig ob er verschoben wurde oder nicht - kommen. So bietet z.B. der Hersteller Sophos als britisches Unternehmen Antiviren-Lösungen und

Mobile Device Management an. Erfolgt der Austritt Großbritanniens aus der EU, handelt es sich aus rechtlicher Sicht um einen Drittstaat, für den kein sog. Angemessenheitsbeschluss der EU vorliegt. Damit stünde Großbritannien wie Solmecke et al. anführen auf einer Stufe mit Staaten wie China oder Russland (2018, S.68). Damit gelten erheblich Restriktionen, was Datentransfers dorthin angeht. EU-Schutzstandards müssten entweder durch Zertifizierer bestätigt oder durch Verträge zwischen den beteiligten Parteien ausgehandelt werden, die Standardschutzklauseln enthalten (Solmecke et al., 2018, S.68). Somit bietet sich auch hier noch reichlich Bedarf an weiterer Forschung.

10.4 Schwierigkeiten mit den technischen Funktionsprinzipien

Zwecks Verständnis, warum die Auswirkungen massiv sind, wurde auf die Funktionsweise des Internets eingegangen. Was Web-Präsenzen anbelangt, ist in technischer Hinsicht zwecks Abruf, die IP-Adresse erforderlich. Eine IP-Adresse kann dabei Personen zugeordnet werden und fällt somit unter die EUDSGVO. Werden zudem noch Spuren im Web hinterlassen von der hinter einer IP steckenden realen Person, was durch die erwähnten Cookies geschehen kann, durch Abspeichern der IP bei Bestellungen in Online-Shops, bei Registrierungen zu Newslettern und dergleichen, liegt in jedem Fall eine Datenverarbeitung vor. Diese Verarbeitung muss einer Person jedoch jedes Mal im Vorfeld derer Erhebung zur Kenntnis gebracht werden. Die Person muss über den Zweck der Datenerhebung informiert werden, dies betrifft konkret die vielfach seit Inkrafttreten der EUDSGO faktisch auf allen Webseiten zu findenden Cookie-Hinweise, die man entweder zu akzeptieren hat, widrigenfalls die Seite nicht ordnungsgemäß funktionieren könnte. Damit sind zugegebenermaßen durch die EUDSGVO erhebliche Komforteinbußen einhergegangen.

10.5 Wurde die EUSDVO ihrer Aufgabe gerecht?

Letztlich bleibt abzuwarten, ob die EUDSGVO ihrer Aufgabe gerecht wird. Bisher ist nämlich wenig davon bekannt, wonach die breite Masse gegen unzulässige Sammlung von Daten vorgeht. Damit sind technisch implementierte Telemtriedaten in Software, die vor der Zeit des Inkrafttretens der EUDSGVO stammt, aber auch fehlerhaft arbeitende oder Software, die aus Drittstaaten

betrieben wird, gemeint. Die Mittel jedenfalls hat die EUDSGVO den Betroffenen in die Hand gegeben, ebenso die Pflicht für Unternehmen, wie das hier betrachtetet fiktive KMU, sich darauf vorzubereiten, da, wie mehrfach erwähnt, die Strafen existenzbedrohend sind und folglich ein einziger erfolgreiches Verfahren gegen ein Unternehmen sein existentielles Aus bedeuten kann. Seit Edward Snowden weiß man ja, wie Datenschutz mit Füßen getreten wird und einmal im Netz vorhandene Daten von überall aus nach überall hin kopiert werden können. Da sie somit faktisch nicht gelöscht werden können, können sie auch nicht besonders geschützt werden. Die EUDSGVO sorgt hier zumindest für griffigen Datenschutz in der Form, wenn Daten schon nicht geschützt werden können, zumindest über rechtliche Sanktionsmöglichkeiten bei Verstößen regulierend einzugreifen.

Ein Unternehmen sollte es sich überlegen, gegen Datenschutzbestimmungen zu verstoßen und wäre gut beraten, auch aus einem Drittstaat sich an die EUSDVO zu halten, soll es nicht mit Sanktionen belegt werden. Letztlich handelt es sich um eine Art Datenschutz „durch die Hintertür", nicht ihn einzuhalten, sondern Verstöße zu unterlassen Insbesondere in Hinblick auf die Blockchain-Technologie, wo bekanntlich sämtliche Transaktionen weltweit verteilt auch auf Rechnern Privater landen, ergeben sich interessante Forschungsansätze. Die Blockchain stellt dabei die Grundlage für Crypto-Währungen wie auch Smart Contracts dar. Besonders bei Smart Contracts lohnt es sich, diese einmal von den datenschutzrechtlichen Bestimmungen her zu betrachten, zumal sie so smart sind, wenn sie einmal veröffentlicht wurden, sie nicht mehr ändern zu können, was bei Verträgen auch sinnvoll, datenschutzrechtlich jedoch bedenklich ist.

kritische Stimmen erblicken in der EUDSGVO durchaus hohe Kostentreiber, schwammige Formulierungen und Rechtsunsicherheit (IT-Rebellen, 2019). Dem ist insofern entgegenzutreten, als hinsichtlich schwammiger Formulierungen bewusst auf die Öffnungsklauseln verwiesen sei, um nationalstaatliche Eigenständigkeit im Sinne sog. integrationspolitischer Schranken der EU nicht auszuhebeln. Was Rechtsunsicherheit betrifft, wird in den nächsten Monaten und Jahren mit richtungsweisenden Urteilen zu rechnen sein, die dann vorgeben,

wie die EUDSGVO letztlich zu interpretieren ist. Strafen sollen dabei abschrecken, aber nicht KMUs treffen, um keine Arbeitsplätze zu gefährden und keine Seiteneffekte in den angrenzenden Wirtschaftssektoren bewirken. Die Kosten der EUDSGVO sind somit als Kosten wie im regulären Change Management für Adaptierungen bestehender Software, bzw. Cloud-Lösungen anzusehen. In der Natur des Menschen liegt es ja, zuerst zu jammern und letztlich doch das Neue zu akzeptieren.

11 Literatur

Abdoulaye, P. A. (2014). Cloud Computing. Advanced Business and IT Strategies to Extract Tangible Value. New York: River Road.

Ahmed, A., Asadullah, S. (2009). Deploying IPv6 in Broadband Access Networks. Hoboken: John Wiley & Sons.

Barath, J. (2017). Optimizing windows 10 logging to detect network security threats. 2017 Communication and Information Technologies (KIT). doi:10.23919/kit.2017.8109438.

Bernhardt, Ute & Ruhmann, Ingo & Schuler, Karin & Weichert, Thilo. (2016). Datenschutzrechtlicher Handlungsbedarf 2016 für die deutsche Politik nach Verabschiedung der EU-DSGVO Eine Empfehlung des Netzwerks Datenschutzexpertise.

Berning, Wilhelm & Meyer, Kyrill & Keppeler, Lutz. (2017). Datenschutzkonformes Löschen personenbezogener Daten in betrieblichen Anwendungssystemen – Methodik und Praxisempfehlungen mit Blick auf die EU-DSGVO. 10.1007/978-3-658-20059-6_12.

BSI (2018). Work Package 4: Telemetry. Version 4.0. Bonn: Federal Office for Information Security.

BSI 1 (2018). IT-Grundschutz Kompendium. Köln: Bundesanzeiger Verlag.

Bundesministerium Digitalisierung und Wirtschaftsstandort WKO (2018). IT Sicherheitshandbuch für kleine und mittlere Unternehmen (9. Auflage). Bad Vöslau: Grasl Druck und Neue Medien GmbH.

Bundesministerium Digitalisierung und Wirtschaftsstandort WKO 1 (2018). IT Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter (9. Auflage). Bad Vöslau: Grasl Druck und Neue Medien GmbH.

Datenschutz-Anpassungsgesetz (2018). Bundesgesetzblatt der Republik Österreich. (NR: GP XXV RV 1664 AB 1761 S.190. BR: 9824 AB 9856 S.871.)

Datenschutzbeauftrager-info.de (2018). Übertragung der Haftung nach DSGVO auf den Arbeitnehmer? Abgerufen von: https://www.datenschutzbeauftragter-info.de/uebertragung-der-haftung-nach-dsgvo-auf-den-arbeitnehmer/.

Datenschutzbehörde Österreich (2018). Impressum & Offenlegung gemäß § 25 des Mediengesetzes. Abgerufen von https://www.dsb.gv.at/impressum-copyright.

Eckhardt, Jens & Kramer, Rudi. (2013). EU-DSGVO — Diskussionspunkte aus der Praxis. Datenschutz und Datensicherheit - DuD. 37. 10.1007/s11623-013-0110-5.

E.O. Elamin, Wadah. M. Alawad, Elwasila Yahya, Abdallah Abdeen, Y.M. Alkasim (2018). Design of Vehicle Tracking System. International

Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE).

Europäische Union (2016). VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Abgerufen von: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE – andere Sprachen unter: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679.

Forensic Files, the. (1996-2011). Als Medical Detectives [TV-Sendung], VOX, 28.04.2019 – 1:20h

Gierschmann, S., Schlender, K., Dr. Stentzel, R. Dr. Veil, W. (Hrsg.) (2018). Kommentar. Datenschutzgrundverordnung. Köln: Bundesanzeiger Verlag GmbH.

Gobeo A., Connor F., Buchanan W. J. (2018). GDPR and Cyber Security for Business Information System. Gistrup: River Publishers.

Gossmann C. (2006). Implementierungsstrategien und Auswirkungen auf Datenschutz- und Urheberrechte vor dem Hintergrund der Internetkommerzialisierung. Diplomarbeit, Universität Wien, Wien.

Haselmann, T. (2012). Cloud-Services in kleinen und mittleren Unternehmen. Nutzen, Vorgehen, Kosten. Dissertation, Westfälische Wilhelms-Universität Münster: Münster.

Help.gv.at (2019). Vorratsdatenspeicherung. Abgerufen von https://www.help.gv.at/Portal.Node/hlpd/public/content/99/Seite.991898.html.

Hubert, T. (2019). First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities. European Data Protection Board: o.V.

Hugos, M., Hulitzky D. (2011). Business in the Cloud. New Jersey: Hoboken.

Hunzinger S. (2018). Das Löschen im Datenschutzrecht. Dissertation, Universität Münster, Baden-Baden: Nomos.

IT-Markt (2017). IT-Markt-Report 2017. Schweiz: Netzmedien AG.

IT-Rebellen (2019). Ziel verfehlt: DSGVO bremst digitale Wirtschaft aus. Abgerufen von: https://it-rebellen.de/2019/05/22/ziel-verfehlt-dsgvo-bremst-digitale-wirtschaft-aus/.

Jamsa, K. (2013). Cloud Computing. SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security, and More. Burlington: Jones & Bartlett Learning.

Katulic, T., Vojkovic, G. (2016). From safe harbour to European data protection reform. 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). doi:10.1109/mipro.2016.7522367.

Keppeler, Lutz & Berning, Wilhelm. (2017). Technische und rechtliche Probleme bei der Umsetzung der DS-GVO-Löschpflichten. Zeitschrift für Datenschutzrecht. 2017. 314-319.

KMU Forschung Austria, Voithofer, P., Hölzl, K., Eidenberger, J. (2012) Bilanzkennzahlen Praxishandbuch. Wien: o.V.

Krishnan, Y. N., Bhagwat, C. N., Utpat, A. P. (2014). Optimizing spanning tree protocol using port channel. 2014 International Conference on Electronics and Communication Systems (ICECS). doi:10.1109/ecs.2014.6892831

Krishnan, S. (2007) Request for Comment 4941. Privacy Extensions for Stateless

Address Autoconfiguration in IPv6. Abgerufen von:

https://tools.ietf.org/html/rfc4941

Kurbos Rainer (1999). Computerausfall - wer zahlt? Wien, Frankfurt:

Wirtschaftsverlag Ueberreuter.

Dr. May, E., Dipl.-Kfm. Fuß, H.J., Dipl.-Kfm. Dürr, G. (2004). Europäischer Wirtschaftsführerschein. Alles für die Zertifikatsprüfung. Braunschweig: westermann druck [sic!] GmbH.

Mayer, T. (2019). Juncker zu Kurz: „Anwürfe gegen EU sind völlig daneben". Abgerufen von https://derstandard.at/2000103198297/Juncker-zu-Kurz-Anwuerfe-gegen-EU-sind-voellig-daneben.

Mayring, P. (2015). Qualitative Inhaltsanalyse. Grundlagen und Techniken. (12. Auflage). Weinheim: Beltz Verlag.

Mewes, B. (2018). CLOUD Act - US-Gesetz für internationalen Datenzugriff und -schutz verabschiedet. Abgerufen von: https://www.heise.de/newsticker/meldung/CLOUD-Act-US-Gesetz-fuer-internationalen-Datenzugriff-und-schutz-verabschiedet-4003330.html?wt_mc=rss.ho.beitrag.atom.

Müller, M. (2018). Die Öffnungsklauseln der Datenschutzgrundverordnung. Ein Beitrag zur Europäischen Handlungsformenlehre. Dissertation, Universität Münster, Münster.

Nas S. (2018). Impact assessment shows privacy risks in Microsoft Office ProPlus Enterprise. Abgerufen von: https://www.privacycompany.eu/en/impact-assessment-shows-privacy-risks-microsoft-office-proplus-enterprise/.

Nas S., Roosendaal A. (2018). DPIA Diagnostic Data in Microsoft Office Proplus. Datenschutzfolgeabschätzung des niederländischen Justizministeriums. Den Haag: o.V.

Obernosterer, B. (2017). Einsatz von Public-Cloud-Services in KMU-Unternehmen und deren Auswirkungen auf Kosten, Sicherheit, Organisation und Wertschöpfungskette. Masterarbeit, FH-Burgenland: Eisenstadt.

Oesterreich.gv.at (2019). Das Recht am eigenen Bild. Abgerufen von https://www.oesterreich.gv.at/themen/bildung_und_neue_medien/internet_und_handy___sicher_durch_die_digitale_welt/7/Seite.1720440.html.

Offener Brief diverser NGOs an den deutschen Bundesminister für Wirtschaft und Energie (2018). Unternehmen und Bürger brauchen starken Schutz elektronischer Kommunikation. Abgerufen von https://www.netzwerk-datenschutzexpertise.de/sites/default/files/eprivacy-appell-altmaier.pdf.

Ohnemus, J. (2018). EU-Datenschutz-Grundverordnung - Unternehmen in Deutschland stehen unter Anpassungsdruck. Abgerufen von: https://www.zew.de/de/presse/pressearchiv/eu-datenschutz-grundverordnung-unternehmen-in-deutschland-stehen-unter-anpassungsdruck/.

ORF Online (2018). Überraschende Entschärfung. Abgerufen von: https://orf.at/v2/stories/2435570/243556/.

ORF Online 2 (2019). DSGVO für Datenschutzaktivisten Schrems zu schwammig. Abgerufen von: https://orf.at/stories/3111315/.

ORF Online 3 (2019). Facebook muss Datenschutz-Dokumente aushändigen. Abgerufen von: https://orf.at/stories/3125249.

Porter, J. (2019). Google fined €50 million for GDPR violation in France. Abgerufen von: https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil.

Retzl, D. (2019). Allgemeine Geschäftsbedingungen der Miss-Webdesign.at

RIS Rechtsinformationssystem (2019). Rechtsinformationssystem des Bundes. Online unter https://www.ris.bka.gv.at

Sathiyaseelan, A. M., Joseph, V., Srinivasaraghavan, A. (2017). A proposed system for preventing session hijacking with modified one-time cookies. 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC). doi:10.1109/icbdaci.2017.8070882.

Schüler, H. P. (2018). Auslaufmodell: Microsoft Cloud Deutschland. Abgerufen von: https://www.heise.de/newsticker/meldung/Auslaufmodell-Microsoft-Cloud-Deutschland-4152650.html.

RA Mag. Schütz, A., Dr. Gneisz, L. (2017). Chancen und Risiken der EU-DSGVO. Wien: o.V.

Shaoqiang Wang, DongSheng Xu, ShiLiang Yan. (2010). Analysis and application of Wireshark in TCP/IP protocol teaching. 2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT). doi:10.1109/edt.2010.5496372.

Soares S., Gallmann M., Basil P. (2017). Data Sovereignty and Enterprise Data Management. Extending Beyond the European Union General Data Protection Regulation. Harrington Park: CreateSpace.

Sokolov, D. AJ (2018). Keine Strafen: Österreich zieht neuem Datenschutz die Zähne. Abgerufen von: https://www.heise.de/newsticker/meldung/Keine-Strafen-Oesterreich-zieht-neuem-Datenschutz-die-Zaehne-4031217.html.

Solmecke, C., Kocatepe, S. (2019). DSGVO für Website-Betreiber. (2. Auflage). Bonn: Rheinwerk Verlag.

Statista (2019). Global spam volume as percentage of total e-mail traffic from January 2014 to December 2018, by month. Abgerufen von: https://www.statista.com/statistics/420391/spam-email-traffic-share/.

Suhr, F. (2019). Das sind die Spam-Top 10. Abgerufen von: https://de.statista.com/infografik/17770/herkunftslaender-von-spam-emails/.

Swire, P, Daskal, J. (2019). Frequently Asked Questions about the U.S. CLOUD Act. Abgerufen von https://www.crossborderdataforum.org/frequently-asked-questions-about-the-u-s-cloud-act/.

Voigt, P., von dem Bussche [sic!], A. (2017). EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch. Springer

Vossen G., Haselmann T., Hoeren T. (2012). Cloud Computing für Unternehmen. Technische, wirtschaftliche, rechtliche und organisatorische Aspekte. Heidelberg: dpunkt.verlag GmbH.

Weinman, J. (2012). Cloudonomics. The Business Value of Cloud Computing. New Jersey: Hoboken.

WKO (2017). ePrivacy-Verordnung. Abgerufen von https://www.wko.at/branchen/information-consulting/werbung-marktkommunikation/ePrivacy-Verordnung.html.

WKO 2 (2018). Informationen zur EU Datenschutzgrundverordnung. Abgerufen von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationen-zur-EU-Datenschutz-Grundverordnung.html.

WKO 3 (2019). Musterdokumente zur EU Datenschutzgrundverordnung. Abgerufen von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Musterdokumente-zur-EU-Datenschutzgrundverordnung.html.

WKO 4 (2019). Muster-Verarbeitungsverzeichnis für Verantwortliche. Abgerufen von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html.

WKO 5 APA Aussendung (2018). Umsetzung der DSGVO – Neues kostenloses Serviceangebot der WKÖ-Bundessparte Handel. Abgerufen von https://www.ots.at/presseaussendung/OTS_20180219_OTS0028/umsetzung-der-dsgvo-neues-kostenloses-serviceangebot-der-wkoe-bundessparte-handel.

WKO 6 (2019). IT-Sicherheitshandbuch für KMU. Abgerufen von https://www.wko.at/site/it-safe/sicherheitshandbuch.html.

WKO 7 (2019). Informationen zur EU Datenschutzgrundverordnung. Abgerufen von https://www.wko.at/site/it-safe/mitarbeiter-handbuch.html.

WKO 8 (2019). EU-Datenschutz-Grundverordnung (DSGVO): Internationaler Datenverkehr. Wann ist der Transfer personenbezogener Daten an Drittländer zulässig? Abgerufen von https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Internationaler-Datenverk.html.

WKO 9 (2018). EU-Datenschutz-Grundverordnung: Verantwortliche und Haftung – FAQ. Abgerufen von: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/eu-dsgvo-verantwortliche-haftung-faq.html.

Zeng, L., Xiao, Y., Chen, H. (2015). Accountable logging in operating systems. 2015 IEEE International Conference on Communications (ICC). doi:10.1109/icc.2015.7249469.

Zhao, F. (2011). On choosing the digital document's file format for long-term preservation. 2011 IEEE 3rd International Conference on Communication Software and Networks. doi:10.1109/iccsn.2011.6013850 S.371.

12 Abbildungs- und Tabellenverzeichnis

13 Abkürzungen

ABGB	Allgemeines bürgerliches Gesetzbuch
BSI	Bundesamt für Sicherheit in der Informationstechnik
CMS	Content Management System
D.h. / d.h.	Das heißt / das heißt
DB	Datenbank
DI	Diplomingenieur
Dipl.-Kfm.	Diplomkaufmann
Dr-	Doktor
DRMS	Digital Rights Management System
EDV	elektronische Datenverarbeitung
et al.	et alii
etc...	et cetera
EUDSGVO	Europäische Datenschutzgrundverordnung
f.	folgende
ff.	fortfolgende
FH	Fachhochschule
GPS	Global Positioning System
Hrsg.	Herausgeber
i.v.m.	in Verbindung mit
KFZ	Kraftfahrzeug
KMU	kleine und mittlere Unternehmen
MBA	Master of Business Administration
MSc	Master of Science
Mrd.	Milliarden
o.a.	oben angeführte(m)
o.V.	ohne Verlag
pos.	positiv(e)
PR	Public Relations
RFC	Request for Comment
S.	Seite
SLA	Service Level Agreement
sog.	sogenannte(r)

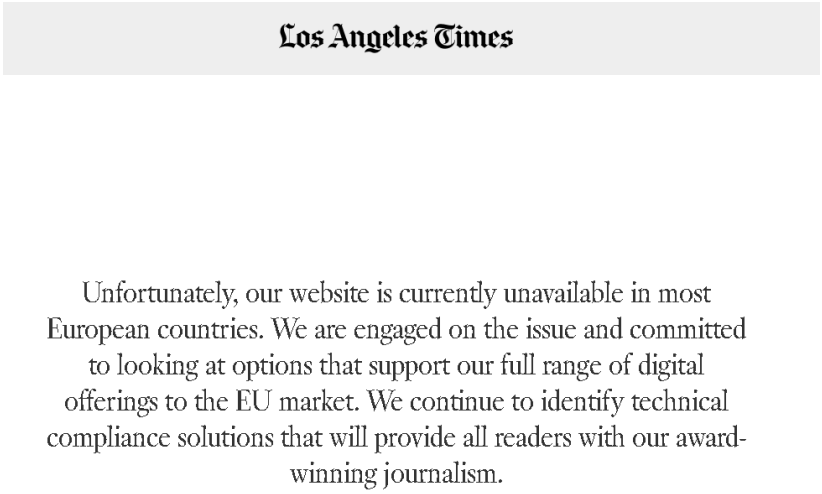
u.a.	unter anderem
USB	Universal Serial Bus
V.a. /v.a.	Vor allem / vor allem
WKO	Wirtschaftskammer Österreich
z.B.	zum Beispiel

14 Anhang

Bevor die Auswirkungen in Zahlen präsentiert werden, sei auf die außerlich wahrnehmbaren Auswirkungen im Web verwiesen. Wie bereits angesprochen, waren etliche Seiten nach Inkrafttreten der EUDSGVO nicht mehr aus Europa erreichbar, wenn sie nicht konform der neuen Verordnung waren.

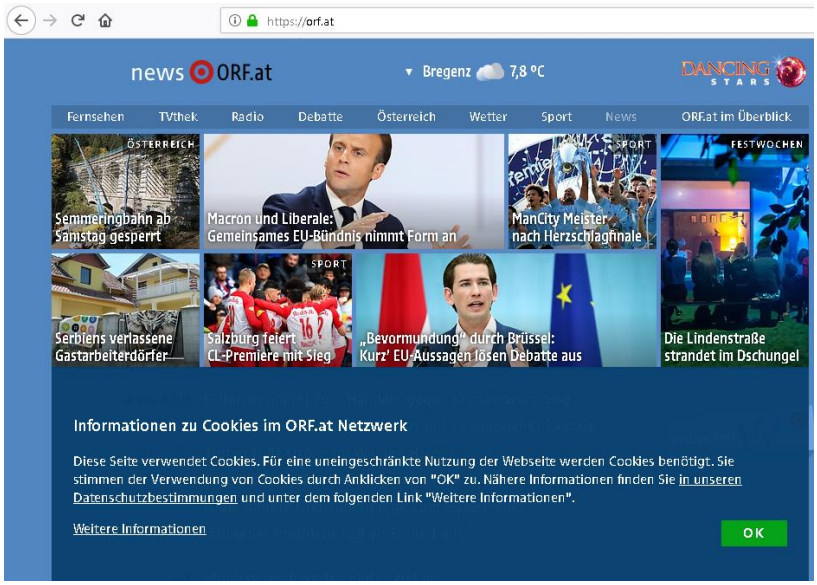
14.1 Auswirkungen konkret

So betraf es u.a. die renommierte L.A Times wie in Anhang-Abbildung eins zu sehen:



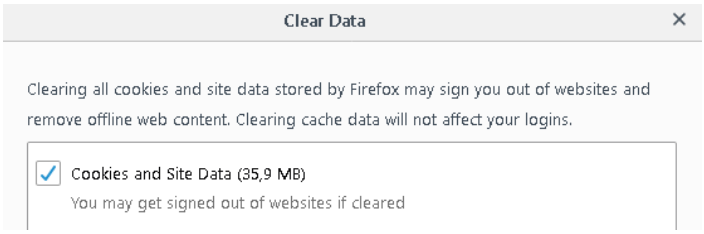
Anh. Abb. 1: L.A. Times nicht erreichbar – Quelle: https://www.latimes.com

Andere Auswirkungen beziehen sich auf Cookie-Hinweise allerorts, wie Anhang-Abbildung zwei zeigt:



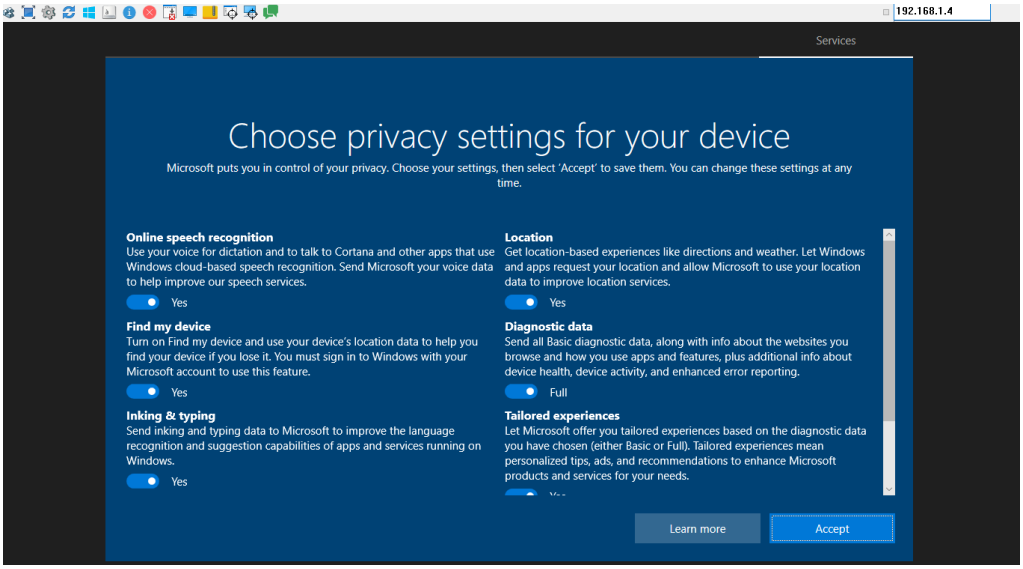
Anh. Abb. 2: Cookie-Hinweis: Quelle: www.orf.at

Genau die Vielzahl an Cookie-Speicherungen und Zustimmungen führt im Webbrowser irgendwann zu einer großen Ansammlung wie in Anhang-Abbildung drei gezeigt und führt zu Verlangsamung:



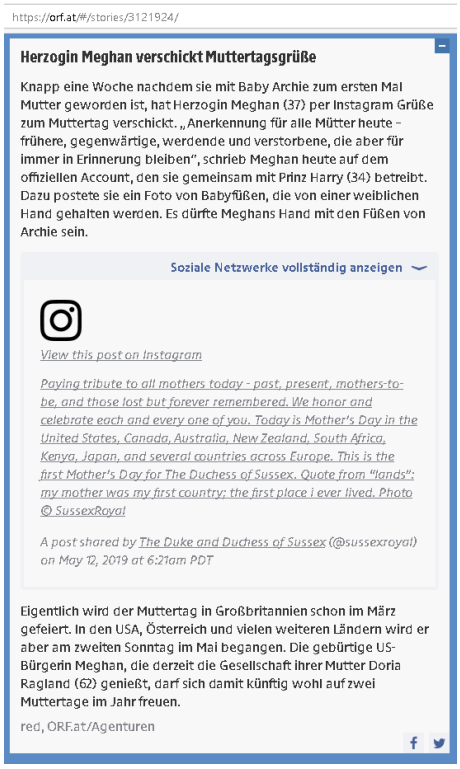
Anh. Abb. 3: Cookies summieren sich / Quelle: Web Browser Firefox V. 67.

Fast 36 MB – nur Cookie-Daten wohlgemerkt sind hier ersichtlich. Vor 25 Jahren wiesen gängige Festplatten mit Windows 3.1 noch eine Gesamtgröße von 40 MB auf. Auch was die angesprochenen Diagnosedaten betrifft, ist derzeit bei einer Neuinstallation von Windows 10 nichts von Privacy by Default zu sehen wie Anhang-Abbildung vier zeigt:



Anh. Abb. 4: Die Standardeinstellungen von Windows 10 – Quelle: Windows 10 V. 1809

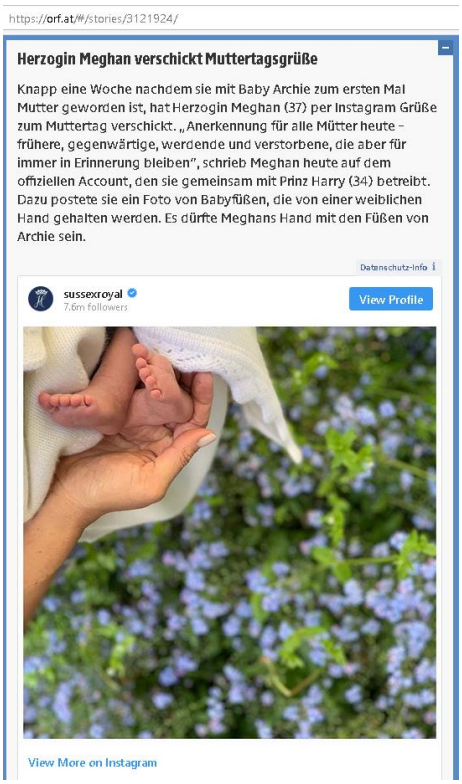
Die Anhang-Abbildungen fünf bis sieben zeigen das mehrstufige Zustimmungsverfahren zur Darstellung von Content sozialer Netzwerke:



Anh. Abb. 5: Stufe 1 soziale Netzwerke einbinden – Quelle: www.orf.at und www.instagram.com

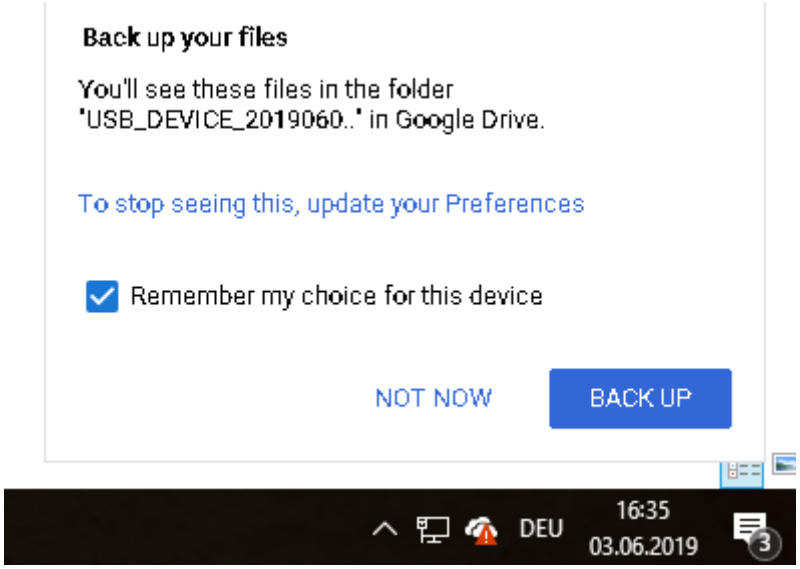
Anh. Abb. 6: Stufe 2 soziale Netzwerke einbinden – Quelle: www.orf.at und www.instagram.com

sowie



Anh. Abb. 7: Stufe 3 soziale Netzwerke einbinden – Quelle: www.orf.at und www.instagram.com

Letztlich zeigt Anhang-Abbildung 8 die Gefahr bei unbedachtem Einstecken externer Datenträger, wie USB-Laufwerken auf modernen Computer-Systemen, die mit Storage as a Service-Lösungen verbunden sind und hier bei standardmäßigen Einstellungen mit dem Upload des Inhaltes beginnen, wenn man die entsprechende Abfrage übersieht oder aus Macht der Gewohnheit wegklickt:



Anh. Abb. 8: Daten externer Datenträger könnten in der Cloud landen

14.2 Auswirkungen im Detail für das fiktive KMU

14.2.1 Definition

Das hier betrachtete fiktive Unternehmen wurde am 2.1.2018 gegründet, baut sich im Laufe des Jahres einen Kundenstamm von 385 Personen auf und startet, da jedes 3. KMU ohne Eigenkapital dasteht (Inhaltsanalyse-Index 31) ebenfalls ohne Eigenkapital. Zwecks Fokus auf das Wesentliche bleiben Abschreibungen und Umsatzsteuern außer Acht, da dies ein reiner Durchlaufposten wäre. Da hier das Jahr 2018 betrachtet wird, bleiben auch Gewinnversteuerung und Rückstellungen außer Acht. Diese würden sich ebenfalls nicht direkt durch die EUDSVO bemerkbar machen, außer man würde Strafen erwarten und deswegen Rückstellungen bilden. Wie gezeigt wird, ist das KMU hervorragend aufgestellt und schafft innerhalb des Jahres 2018 den Verschuldensgrad faktisch gegen 0 zu drücken. Dies liegt an dem Umstand, nach wie vor hohe Preise für Webseiten zu bezahlen, insbesondere durch die 10% höhere Nachfrage wegen der EUDSGVO neben dem operativen Tagesgeschäft.

14.2.2 Die Unternehmensform

Die Gründung des Unternehmens erfolgte als GmbH mit Gründungsbonus, d.h. lediglich mit einer Kapitaleinlage von 5000 Euro. Gründer war eine geschäftsführende Person, die zwecks Miete von Büroräumlichkeiten und Aufbau, bzw. Kauf der IT-Clientinfrastruktur 100.000 € Kredit aufnahm. Das Unternehmen gehört mit 12 Angestellten insgesamt zu den Kleinunternehmen, ist jedoch gerade groß genug, um einen Datenschutzbeauftragten benennen zu müssen, wie in der Arbeit gezeigt wurde. Tätigkeitsbereich ist die Erstellung von Webseiten, die auch die Quelle für den Umsatz darstellen.

Eigene IT-Infrastruktur ist nicht wirklich vorhanden, außer Clients und NAS-Storage-System. Die operative Tätigkeit des Hostings im Sinne von Testen ist outgesourced bei einem IaaS-Anbieter. An Software kommt das Mietmodell für die Adobe Creative Suite hinsichtlich der Grafik- und PR-Abteilung zum Einsatz. Für Development und Datenbanken wird vollumfänglich auf Open Source und CMS gesetzt, weshalb hier keinerlei Kosten anfallen.

In Hinblick auf die Umstellung auf EUDSGVO-Compliance am 25.5.2018 wird bereits Anfang Mai mit entsprechenden Änderungen betreffend des Datenschutzes eine damit beauftragte externe Person betraut und dessen Software, bzw. Beratung in Anspruch genommen. Zu Beginn des Jahres wird jedoch sofort eine Rechtsschutzversicherung abgeschlossen, da es normalerweise bis zu 6 Monate dauert, bis auch tatsächliche Rechtsschutzdeckung eintritt. Dies geht sich praktisch wunderbar aus, da innerhalb der wenigen Tage von 25.5.2018 bis zum 1.6.2018 noch nicht mit einem Rechtsstreit bezüglich der EUDSGVO zu rechnen ist.

Zwecks Vereinfachung werden Abschreibungsposten nicht behandelt. Dies würde auch nicht viel Sinn ergeben, da die Hardware-Ausstattung, für die AfA geltend gemacht werden könnte, sowohl mit also auch ohne EUDSGVO auftreten würde.

Anhang-Tabelle eins zeigt zuerst die Eckdaten von KMUs. Anhang-Tabelle zwei zeigt die Definition des hier verwendeten fiktiven KMUs, während die folgenden Anhang-Tabellen drei bis xx die Kodierbogen-Regeln der Inhaltsanalyse und die Endergebnisse mit den Auswirkungen der EUDSGVO auf das Webdesing-KMU zeigen. Die eigentlichen Inhaltsanalysedaten selbst, sind dabei nicht abgedruckt, sondern online verfügbar (www.gossmann.at), bzw. auf der CD zur vorliegenden Masterarbeit.

Definition gem. WKO-Österreich KMU				
	Mitarbeiter	**Umsatz**	**Bilanzsumme**	**Eigenständigkeit**
Kleinstunternehmen	bis 9	max. 2 Mio. €	max. 2 Mio. €	Kapitalanteile oder Stimmrechte im Fremdbesitz unter 25%
Kleinunternehmen	bis 49	max. 10 Mio. €	max. 10 Mio. €	
Mittlere Unternehmen	bis 249	max. 50 Mio. €	max. 43 Mio. €	
Großunternehmen	ab 250	mehr als 50 Mio. €	mehr als 43 Mio. €	

Anh. Tab. 1: KMU-Defintion (Quelle: https://www.wko.at/service/zahlen-daten-fakten/KMU-definition.html)

	Metriken	Berechnung	Aussage
	Cashflow (May, Fuß, Dürr, 2004, S. 58)	Erträge - Aufwendungen [+ Abschreibungen - Rückstellungen, hier nicht verwendet]	zur Verfügung stehende Mittel
	Verschuldensgrad (May, Fuß, Dürr, 2004, S. 48)	Fremdkapital / Eigenkapital	Prozentsatz der Verschuldung
Personalkosten in Prozent der Betriebsleistung (Personalintensität) (KMU Forschung Austria, 2012, S.75)		(Personalaufwand - hier Lohn gesamt / Gesamtleistung - hier Umsatz) x 100	Auslastung des Personals
	Return on Sales (KMU Forschung Austria, 2012, S.29)	Gewinn / Umsatz	erwirtschafteter Gewinn pro eingenommenem €
	Return on Investment (May, Fuß, Dürr, 2004, S. 52)	(Gewinn / Gesamtkapital) * 100	erwirtschafteter Gewinn pro € des Gesamtkapitals

Begründung für Wahl obiger Metriken:	diese spiegeln die finanzielle Situation eines Unternehmens hervorragend wider. Cashflow und Verschuldensgrad die Finanzlage, Personalkosten in Prozent der Betriebsleistung die effektive Arbeitsweise, also wie optimal Personal eingesetzt wird, während Return on Sales und Investment den Profit widerspiegeln

	Codierregeln
1	Suche nach Begriffen, in denen die Metriken, bzw. Werte mit denen sich diese berechnen lassen, vorkommen. Stehen Werte dabei: heranziehen.
2	Suche nach Begriffen, in denen die Metriken vorkommen, stehen keine Werte dabei, versuche sie aus dem Text zu erschließen.
3	Lassen sich Werte mehreren Metriken zuordnen, betrachte sie als Gesamtheit, da es ein Paketangebot ist, das alles umschließt.
4	Lassen sich Informationen nicht oder nur schwer zuordnen, dann verwerfen und andere Quelle suchen

	Ankerbeispiele dazu
1	Die auf die Entwicklung und Betreuung von Webauftritten spezialisierte Web 2.0 GmbH erzielt mit acht Mitarbeitern einen Umsatz von 890.000 € und einen Jahresüberschuss von 210.000 €.
2	Der Mitarbeiter muss etwa das 2,5-fache der für ihn anfallenden Personalkosten erwirtschaften.
3	Webdesign BUSINESS 2480, Webdesign PLUS ab 3280, Das Neugründer-Paket 2980
4	N/A

Anh. Tab. 2: Die Kodierregeln der Inhaltsanalyse (eigene Darstellung)

Basisdaten	Codierbogen-Index Unternehmen:	"FiktiWeb"
N/A	Beträge in	€
N/A	Gründung	2.1.2018
N/A	**Personalstand**	**12**
10	**Kunden**	**385**
17	Rechtsform	GmbH
27	Typ	KMU
31	**Eigenkapital**	**0**
31	**Fremdkapital**	**100.000**

Anh. Tab. 3: Eckdaten des fiktiven Webdesign-KMU (eigene Darstellung)

	Codierbogen-Index	Anschaffung	Anzahl	monatlich	jährlich	einmalig	Summe	DSGVO-Auswirkung	finanzielle Auswirkungen	Anmerkung
Einmalkosten	17	GmbH-Stammeinlage (Gründungsprivileg)	1			5.000,00	5.000,00	nein	nein	mit Gründungsbonus, daher nur 5000 Stammeinlage
Ausstattung	55	Möbel Computertische	11			375,90	4.134,90	nein	nein	11 PCs für 11 Mitarbeiter ohne Reinigungskraft
	63	Flyer 4000 Stk. Werbung	1			35,99	35,99	jein	persönliche Namen von Mitarbeitern, Bilder	
	64	Bürostuhl	11			95,99	1.055,89			
	N/A	Unvorhergesehenes	1			2.000,00	2.000,00			
	1	Visitenkarten 500 Stk.	1			18,99	18,99	nein	nein	
Speicher	5	USB-Sticks mit Werbelogo und Infos zum I	500			8,82	4.410,00	nein	nein	dient der Werbung und vielleicht bringen Kunden darauf gleich Material
	32	USB-Sticks	24			39,94	958,56	nein	nein	für jeden Mitarbeiter 2
	77	Blu Ray Rohlinge 50er Pack	5			40,92	204,60	jein	richtige Daten brennen, nicht irrtümlich andere	für Kunden zwecks Endauslieferung der Seiten darauf
Netzwerk	20	Switch	1			3.569,00	3.569,00	jein	Hardware-Traps	
	3	Netzwerk CAT 7 Kabeln 10m	60			14,90	894,00	nein	nein	
	46	CAT-Dosen	2			45,80	91,60	nein	nein	
	56	CAT 7-Kabel (Mauer)	2			115,80	231,60	nein	nein	
	57	Netzwerkschrank	1			199,90	199,90	nein	nein	
	65	Eletrkoinstallation Netzwerk	1			6.195,00	6.195,00	nein	nein	
	8	Hardware Firewall Sophos XG 210	1			1.264,38	1.264,38	nein	nein	
	33	WLAN-Access-Points	2			234,95	469,90	nein	nein	zwecks besserer Abdeckung gleich 2
	22	IP-Telefon	11			72,34	795,74	jein	Aufzeichnung: nicht Kunde muss nein sagen	
	28	Mitarbeiter Smartphones	12			169,90	2.038,80	jein	nur im Klagsfall	Whatsapp und Datenschutzeinstellungen prüfen
Drucker	67	Fax(drucker)	1			156,90	156,90	nein	nicht öffentlich unbeaufsichtigt lassen - Speicherfax	nebenbei als Zweitdrucker und Reservescanner für Multidrucker
	2	Multifunktions-Drucker-Scanner	1			3.190,00	3.190,00	jein	nur im Klagsfall (Festplatte drinnen)	verschlüsselt drucken
	4	Kopier- und Druckpapier 5000 Blatt	1			42,99	42,99	nein	nein	
Clients	21	PC-SETs	11			299,00	3.289,00	nein	nein	Reinigungskraft braucht keinen PC
	60	Aufrüstung auf 16 GB Speicher	2			82,99	165,98	nein	nein	für Grafik und Marketing
	34	Zusatzmonitore	8			149,90	1.199,20	nein	nein	für Leitung, Admins, Grafik, Marketing, Developer
	59	Laptop Leitung	1			1.549,00	1.549,00	jein	technische Maßnahmen - Bitlockerverschlüsselung	
	78	Dockingstation für Laptop Leiter	1			225,00	225,00	nein	nein	
	79	Maus und Tastatur für Dockingstation	1			24,99	24,99	nein	nein	
	69	Lautsprecher	12			14,99	179,88	jein	Mithören von Gesprächen	jedem PC und dem Leitungs-Laptop für VoIP Desktopconrol
	70	Headsets	12			31,99	383,88	jein	Mithören von Gesprächen	jedem PC und dem Leitungs-Laptop für Skype z.B.
	71	Webcams	11			21,99	241,89	jein	Mithören von Gesprächen, aut. Upload von Bildern in Sa	in Laptop ist eine eingebaut darum 11, für Videokonferenzen mit Kunden
	76	Maus und Tastatur-Handauflage	12			19,99	239,88	nein	nein	zur Gesundheit der Mitarbeiter für alle PCs und den Laptop
	75	Blu Ray Brenner	1			90,63	90,63	nein	nein	für Kunden zwecks Endauslieferung der Seiten
Software	61	Backup-Software für PC 3er-Lizenz	4			26,99	107,96	ja	welche Daten wie lange - Löschverpflichtung	4*3er-Lizenz für 11 Mitarbeiter (=11 PCs u. 1 Laptop Leitung) = 12 Lizenzen
	7	Otris Privacy Einzellizenz	1			289,00	289,00	ja	-289	

Software	61	Backup-Software für PC 3er-Lizenz	4			26,99	107,96	ja	welche Daten wie lange - Löschverpflichtung	4*3er-Lizenz für 11 Mitarbeiter (=11 PCs u. 1 Laptop Leitung) = 12 Lizenzen
	7	Otris Privacy Einzellizenz	1			289,00	289,00	ja	-289	
Server	18	Server Development Einrichtung	1			99,90	99,90	jein	prüfen, ob EUDSGVO-konform (LOGs)	120 GB RAM, 4x1 TB Harddisc, 24 Cores, eigene Betriebssysteme möglich
	18	Testserver f. Kunden Einrichtung	1			99,90	99,90	jein	prüfen, ob EUDSGVO-konform (LOGs)	120 GB RAM, 4x1 TB Harddisc, 24 Cores, eigene Betriebssysteme möglich
	18	Server Verwaltung / Kunden	1			99,90	99,90	jein	prüfen, ob EUDSGVO-konform (LOGs)	120 GB RAM, 4x1 TB Harddisc, 24 Cores, eigene Betriebssysteme möglich
	19	NAS-Storage-Systeme	2			1.346,95	2.693,90	nein	nein	
	14	Ventilator für Technikschrank (NAS)	1			80,18	80,18			
	80	Thermometer für Technikschrank	1			191,00	191,00			
	62	NAS-Festplatten	32			171,90	5.500,80			2 NASse voll bestückt mit 16x4 TB-Platten auf RAID 6 - 56 TB mit 2 ausfallbaren Platten
	58	Fachboden	2			19,48	38,96	nein	nein	für NASse
Sonstiges	N/A	Kleinkram (Schreibzeug, Kugelschreiber, E	1			500,00	500,00	nein	nein	
	54	Schulungskosten Personal	1			3.120,00	3.120,00	ja	-3120	
	68	USVs	12			149,90	1.798,80	nein	nein	jedem PC und für den Technikschrank (Switch / Firewall / Aps / NAS) seine Desktop-USV
					CAPEX	Summe	59.168,37			

jährliche OPEX

Domain	12	Domain AT	1		14,90		14,90	jein	RIPE-Datenbank auf korr. Daten checken	für eigenen Webauftritt
	13	Domain EU	1		14,90		14,90	jein	RIPE-Datenbank auf korr. Daten checken	für eigenen Webauftritt
					j. OPEX	Summe	29,80			

mtl. OPEX

Services	11	Mietkosten für Räumlichkeiten	1	1757,00			1757,00	nein	nein	
	6+24+25+48+49	Stromkosten	1023,36	0,07			69,24	nein	nein	12 PCs (0,36 kw), NAS (0,05 kw), Switch (~0,37 kw), Licht, Telefone, Laptop und Handys laden ~1 kw / h) - 8 Stunden - 20,5 Werktage
	26	Stromkosten Grundgebühr	1	15,00			15,00	nein	nein	
	73	ELBA Business	1	224,00			224,00	ja	Verschlüsselung prüfen, SLAs, Bankdaten	elektronik Banking für Sekretariat
	74	Kreditrückzahlung	1	1321,33			1321,33	nein	nein	
	36	Rechtsschutz	1	100,00			100,00	nein	Rechtsschutz kann man immer brauchen	
Datennetz	30	Mobilnetztarif	12	29,90			358,80	nein	nein	
	23	Internet-Zugang	1	79,90			79,90	nein	nein	
	66	redundantes Festnetzinternet	1	19,00			19,00	nein	nein	hauptsächlich wegen Faxunterstützung
	37	unlimitiertes Hosting und Datenbanken	1	9,90			9,90	jein	Logs abdrehen oder Zustimmung einholen	um ungestört Entwickeln zu können
	9	Sophos Firewall Lizenzkosten	1	54,27			54,27	jein	Brexit ? / Sophos ist ein brittisches Unernehmen	
Server	18	Server Development	1	199,99			199,99	jein	nein, nur Prozessänderung	für IT zur Entwicklung
	18	Testserver f. Kunden Einrichtung	1	199,99			199,99	jein	nein, nur Prozessänderung	für Demo und Abnahme durch Kunden
	18	Server Verwaltung / Kunden	1	199,99			199,99	jein	nein, nur Prozessänderung	
	72	Server-Housing	1	89,90			89,90	ja	SLA prüfen, Zertifizierung, Verschlüsselung	Outsourcing der Backups zu einem Rechenzentrum auf eigenem NAS
Cloud-Software	35	Office 365 Business SaaS	11	10,50			115,50	jein	Datenschutz prüfen, im Klagsfall Probleme	für Anlieferung von Dateien durch Kunden und Bürowecke
	29	Grafiksuite SaaS	2	59,99			119,98	jein	Datenschutz prüfen, Bildrechte beachten	Grafikdesigner und Marketing-Abteilung
	15	zusätzliche Datenschutz-Mietsoftware	1	49,90			49,90	ja	-49,9	

Personal											
	38	Geschäftsführung		1	2911,00			2911,00	ja		
	39	Developer		3	2634,00			7902,00	ja	Verantwortung beachten	GmbH-Gründer
	40	Datenbank-Analyst		2	2634,00			5268,00	ja	Prozesse ändern	Kerngeschäft, darum 3
	41	Grafikdesigner		1	2383,00			2383,00	ja	Datenminimierung beachten	auch für CMS und Development
	42	Sekretariat		1	2383,00			2383,00	ja	Bildrechte beachten	für PR und Development
	44	Marketing und PR		1	2383,00			2383,00	ja	E-Mail-Verkehr	für Kundenkontakt und Kommunikation
	43	Systemadministratoren		2	2634,00			5268,00	ja	Nie vollständig rückverfolgbar durch Double-Opt-In	für Marketing (PR)
	45	Reinigungspersonal		1	1764,00			1764,00	ja	Implementierungen von Software und Prozessen	sowohl on-Premises wie IaaS-Cloud
						Summe		35.245,69		Aufklären bei Datenspeicherung bei Zeiterfassung	

Personal ab Mai									
	16	ext. datenschutzbeauftragte Person		1	400,00			400,00	ja

erwartete mtl. Einnahmen aus Webdesign									
	10+51		Standard	20	2250,00			45000,00	nein
	10+52		Professional	10	2850,00			28500,00	nein
	10+53		Onlineshop	2	4850,00			9700,00	nein
	10+47+51		Standard	2	2250,00			4500,00	ja
	10+47+52		Professional	1	2850,00			2850,00	ja
	10+47+53		Onlineshop	0,2	4850,00			970,00	ja

	-400,00		
nein			
nein			
nein			
ja	4500	10% Auftragsplus wegen DSGVO	
ja	2850	10% Auftragsplus wegen DSGVO	
ja	970	10% Auftragsplus wegen DSGVO, muss auf das Jahr verteilt betrachtet werden, daher 0,2	

385 / 12 Monate = ~33 , jeder Bisstsich nicht eine prof. Seite oder einen Onlineshop erstellen

Anh. Tab. 4 (3-seitig): Auswirkungen der EUDSGVO in Zahlen (eigene Darstellung)

Anh. Tab. 1: Eckdaten des fiktiven Webdesign-KMU (eigene Darstellung)

2018	Einnahmen	Ausgaben	Kasse	Schulden
Jan	91.520,00	94.443,86	97.076,14	98.678,67
Feb	91.520,00	35.245,69	153.350,46	97.357,34
Mar	91.520,00	35.245,69	209.624,77	96.036,01
Apr	91.520,00	35.245,69	265.899,09	94.714,68
May	91.520,00	35.645,69	321.773,40	93.393,35
Jun	91.520,00	35.645,69	377.647,72	92.072,02
Jul	91.520,00	35.645,69	433.522,03	90.750,69
Aug	91.520,00	35.645,69	489.396,35	89.429,36
Sep	91.520,00	35.645,69	545.270,66	88.108,03
Oct	91.520,00	35.645,69	601.144,98	86.786,70
Nov	91.520,00	35.645,69	657.019,29	85.465,37
Dec	91.520,00	35.645,69	712.893,60	84.144,04
Summe	1.098.240,00	485.346,40		

2018	Cashflow	Verschuldensgrad	Personalintensität	RoS	RoI
Jan	-2.923,86	100,00	0,33	-0,03	-3,01
Feb	56.274,31	1,79	0,33	0,61	36,70
Mar	56.274,31	0,88	0,33	0,61	26,85
Apr	56.274,31	0,58	0,33	0,61	21,16
May	55.874,31	0,44	0,34	0,61	17,36
Jun	55.874,31	0,35	0,34	0,61	14,80
Jul	55.874,31	0,29	0,34	0,61	12,89
Aug	55.874,31	0,25	0,34	0,61	11,42
Sep	55.874,31	0,22	0,34	0,61	10,25
Oct	55.874,31	0,19	0,34	0,61	9,29
Nov	55.874,31	0,17	0,34	0,61	8,50
Dec	55.874,31	0,16	0,34	0,61	7,84
Summe	612.893,60				

Anh. Tab. 5: Die Metriken in Zahlen (eigene Darstellung)

	mit EUDSGVO		ohne EUDSGVO		mit EUDSGVO		ohne EUDSGVO		mit EUDSGVO		ohne EUDSGVO		mit EUDSGVO		ohne EUDSGVO	
	Datenbank				Grafik-SW				Hosting				Development			
Cashflow	ohne, da Open Source	1	ohne, da Open Source	1	bleibt gleich	1	bleibt gleich	1	bleibt gleich	1	bleibt gleich	1	höherer Aufwand	0	geringerer Aufwand	1
Verschuldensgrad	keine Kosten	1	keine Kosten	1	bleibt gleich	1	bleibt gleich	1	bleibt gleich	1	bleibt gleich	1	höherer Aufwand	0	geringerer Aufwand	1
Personalintensität	um 0,01 höher ab Mai	1	geringer um 0,01	0	Bildrechte beachten	0	keine Strafen	1	Mehraufwand SLAs	0	keine Kosten	1	höher	1	geringer	0
Return on Sales	höherer Erwirtschafteter Gewinn und 10% Umsatzplus	1	kein Umsatzplus	0	Aufträge für Verpixelungen und Prüfungen	1	bleibt gleich	0	pos. Reputation	1	weniger Vertrauen	0	Umrüstkostenaufträge	1	keine Zusatzaufträge	0
Return on Investment	fällt ab wegen Gewinnhortung	1	fällt wegen Gewinnhortung	1	keine Auswirkung	1	bleibt gleich	1	Mithaftung	0	nicht unbedingt Rechtsschutz	1	einfache Zusatzaufträge durch Umrüstung	1	keine Umrüstung und daher keine Kuden	0
Spalte und Summe der Felder	**mit EUDSGVO**	5	**ohne EUDSGVO**	3	**mit EUDSGVO**	4	**ohne EUDSGVO**	4	**mit EUDSGVO**	3	**ohne EUDSGVO**	4	**mit EUDSGVO**	3	**ohne EUDSGVO**	2

Ergebnis im Endeffekt	
Punkte EUDSGVO	**7**
Punkte ohne EUDSGVO	**5**
Auswirkungen daher	**positiv**

Anh. Tab. 6: Die qualitativen Auswirkungen (eigene Darstellung)

Eidesstattliche Erklärung

Hiermit erkläre ich ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Ich erkläre außerdem, dass die vorliegende Arbeit bei keiner anderen Institution (Fachhochschule, Universität, Pädagogische Hochschule oder vergleichbare Bildungseinrichtung) zur Erlangung eines akademischen Grades eingereicht wurde.

Ort, Datum	Unterschrift