



IHR EXTERNER DATENSCHUTZBEAUF- TRAGTER INFORMIERT.

Online Magazin—Ihr externer Datenschutzbeauftragter Gehrmann

Oktober 2020 | Ausgabe 1

Das Ziel unseres Online Magazins

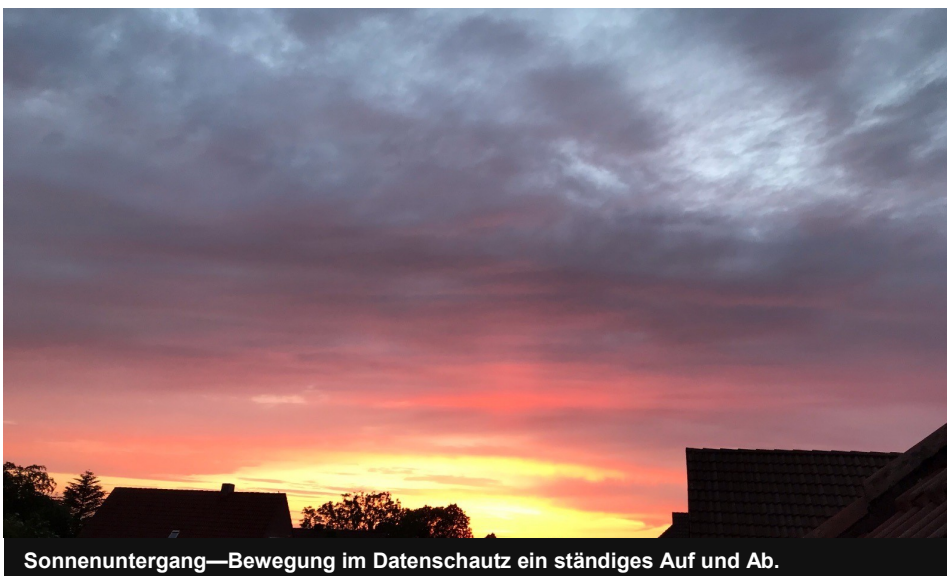
Ab sofort möchten wir Sie liebe Leserin und lieber Leser über die aktuellen Ereignisse rund um den Datenschutz und Datensicherheit regelmäßig informieren. Dieses Online Magazin ist, wird und bleibt kostenfrei und hat zum Ziel komplexe neue Gegebenheiten für Jedermann leicht verständlich und überzeugend zu erläutern. Tipps für zukünftige Verhaltensweisen und Möglichkeiten zum Schutz der eigenen persönlichen Privatsphäre werden ebenfalls mit auf den Weg gegeben. Natürlich darf eine gewisse Portion an Würze durch wohldosierten Sarkasmus zur Erheiterung aller nicht fehlen.

Unsere Top-Themen sind:

- ◆ Der Datenschutzbeauftragte
- ◆ Thunderbird mit PGP-Verschlüsselung
- ◆ Facebook: Einführung von Verschlüsselung
- ◆ Bußgelder in Deutschland

"Künstliche Intelligenz gibt es nicht ohne ein Bewusstsein. Und hätte Sie ein Bewusstsein, dann wäre es Intelligenz ohne künstlich zu sein."

- Markus Don Alfred Gehrmann -



Sonnenuntergang—Bewegung im Datenschautz ein ständiges Auf und Ab.

Inhalt dieser Ausgabe

- Der Datenschutzbeauftragte
- Datenverschlüsselung bei Facebook und Mozilla
- Der Mytos ... Visitenkarte
- Bußgelder & Datenschutz-Verstöße
- EuGH: Cookies
- Wichtige Termine
- Was ist..?
- Tool-Tipps
- Links
- Der Datenschutz-Witz



Datenschutz: Der Beauftragte seine Aufgaben und Missverständnisse

Der Datenschutzbeauftragte

Was sind seine Aufgaben - Wir räumen auf mit Missverständnissen.

Seit Einführung der DSGVO am 25. März 2018 halten sich stark die Irritationen darüber welche Aufgaben der Datenschutzbeauftragte inne hat. Das gilt gleich wohl für den internen als auch für den externen. Obgleich sich die Aufgaben an sich in nichts unterscheiden. Es ist lediglich die Stellung innerhalb des Unternehmens und die Haftbarkeit.

Gerade klein und mittelständische Unternehmen fühlen sich überfordert im Verständnis darüber was die DSGVO von ihnen verlangt und wie sie dem gerecht werden sollen. Denn ihre Kernaufgabe ist das Tagesgeschäft, wenn auch gleich wohl der Datenschutz nicht neu ist sondern schon immer galt. Mit in Kraft treten der DSGVO werden Vergehen erstmalig sanktioniert und das nicht in unerheblichen Maße. Die Bußgelder sprengen des Öfteren die Millionen-grenze. Daher ist verständlich das die Unternehmen natürlich Angst vor Bußgeldern haben da sie ihr eigenes unternehmerisches Risiko in Hinblick auf den erforderlichen Datenschutz und die Datensicherheit von personenbezogenen Daten nicht kennen.

Was ist ..? E-Evidence

e-Evidence ist eine EU-weite Verordnung die die Herausgabe von personenbezogenen als auch ermittlungsrelevanten Daten bei Strafverfolgung von Unternehmen erzwingen soll. Das bedeutete das zum Beispiel deutsche Internet- und Serviceprovider Anfragen aus dem europäischen Ausland entsprechend bearbeiten und personenbezogene Daten von Betroffenen herausgeben müssen die evtl. nach deutschem Recht keine Straftat begangen haben.

Die Beteiligung inländischer Justizbehörden ist bis jetzt nicht vorgesehen. Diese treten erst dann aktiv in Erscheinung wenn sich ein Unternehmen weigert angeforderte Daten heraus zu geben.

Die Verordnung ist noch nicht verabschiedet. Es existiert lediglich ein Entwurf der nicht zu kontrollieren bzw. überwachen ist.



Kooperatives Arbeiten

Der besondere Schutz für Kinder

Der Erwägungsgrund 39 der DSGVO beschreibt den besonderen Schutz für Kinder auf Grund fehlender Erfahrungen und weniger entwickelten kognitiver Fähigkeiten.

Dieser Schutz gilt primär für Webermaßnahmen als auch das Profiling.

Die IWGDPT, ein Arbeitskreis unterschiedlicher Datenschutzbehörden erstellt entsprechende Papiere zu bestimmten Themen die allerdings weniger rechtlich bindend und mehr als Empfehlung zu verstehen sind.

In diesen Papieren der Arbeitsgruppe geht es darum das der Betroffene von einzuholenden Einwilligungen des Kindes absieht und auch dafür sorgt das dem Schutz des Kindes genüge getan wird.

Das hält die Eltern jedoch nicht von der Pflicht ab möglichst gemeinsam mit ihren Kindern das Internet zu erforschen und sie auf die bestehenden Gefahren hinzuweisen.

Eltern müssen durchaus die Nutzung des Internets ihrer Kinder kontrollieren und Schutzmaßnahmen einrichten.



Datenschutz und Datensicherheit

Für den beruflichen und unternehmerischen Alltag kann das schnell zu viel werden, wenn man sich nicht schon eh seit Jahren damit befasst. Daher ist der Datenschutzbeauftragte derjenige der unterstützend beratend tätig wird. Er schließt die Lücke mit fachlichem und rechtlichem Wissen um das erforderliche Maß an DSGVO-Konformität für ein Unternehmen zu erreichen.

Keinen Datenschutzbeauftragten ist kein Grund nicht für Datenschutz personenbezogener Daten seiner Mitarbeiter und Mitarbeiterinnen, Kunden und Lieferanten zu sorgen. Ganz im Gegenteil, es ist und bleibt die höchste rechtliche Pflicht.

Tatsächlich sind die Aufgaben eines Datenschutzbeauftragten in Artikel 39 DSGVO klar geregelt.

Diese sind:

- die Beratung in allen Datenschutzbelangen,
- die Sensibilisierung von Mitarbeitern in Bezug auf Datenschutz,
- die Zusammenarbeit mit der Datenschutzbehörde/Aufsichtsbehörde,
- er ist direkter Ansprechpartner für Betroffene,
- Überwacht und Unterstützt bei einer Datenschutzfolgenabschätzung, sofern ein Unternehmen diese zu erstellen hat.

Was hingegen nicht seine Aufgabe ist, ist die Umsetzung von datenschutztechnischen und organisatorischen Maßnahmen. Auch



Datenschutz: Der Beauftragte seine Aufgaben und Missverständnisse

trägt er nicht die Verantwortung sondern diese obliegt ausschließlich der Geschäftsführung.

Welche Pflichten unterliegen dabei der Geschäftsführung in Hinblick auf den Datenschutzbeauftragten?

- Sie stellt sicher das der Datenschutzbeauftragte rechtzeitig in alle personenbezogenen Belange des Unternehmens eingebunden ist.
- Sie unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben.
- Sie ist dem Datenschutzbeauftragten gegenüber nicht Weisungsberechtigt, auch kein anderer Mitarbeiter des Unternehmens.
- Der Datenschutzbeauftragte darf wegen seiner Zweckerfüllung nicht Abberufen oder benachteiligt werden.

Somit habe ich hier einmal beide Seite klar gestellt wie es die DSGVO vorsieht.

Somit ist klar, der Datenschutzbeauftragte berät, weist auf Verbesserungen nach entsprechender Analyse und wirkt auf dessen Ausbesserung aktiv hin. Ob das Unternehmen schließlich seiner Weisung und Empfehlung folgt, ist ihre eigene Entscheidung. Sie muss nicht, doch sie wäre gut beraten, würde sie den Empfehlungen des Datenschutzbeauftragten folgen.

Natürlich unterliegt der Datenschutzbeauftragte gewissen Pflichten die auch er genauestens befolgen sollte um nicht unnötig Situatio-

Was sind personenbezogene Daten?

Unter dem Begriff "personenbezogene Daten" versteht der Gesetzgeber alle Informationen einer identifizierten oder identifizierbaren natürlichen Person wie zum Beispiel:

- den Namen, Vor- und Nachnamen einer Person,
- Geburtsdaten
- Anschrift und Herkunft,
- Kontaktmöglichkeiten wie z. B. Emailadresse, Mobilnummer, Festnetztelefon, Instant Messaging,
- Merkmale zu genetischen, psychischen, physischen, wirtschaftlichen, kulturellen oder sozialen Identität.

Beschrieben wird das in Artikel 4 (Begriffsbestimmungen) der DSGVO.

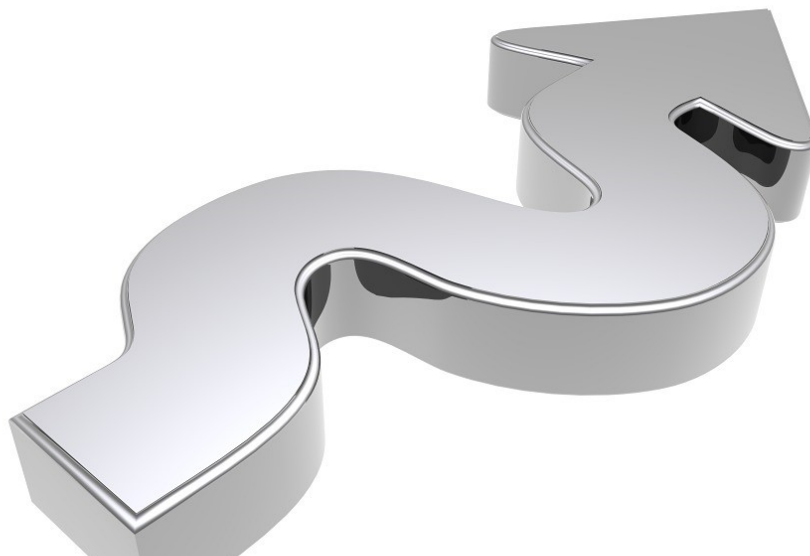


Erfolgreich Datenschutz betreiben.

Warum ist Datenschutz so wichtig ?

Die technischen Neuerungen und Weiterentwicklungen unserer Zeit bringen viel Bequemlichkeit und Nutzen mit sich. Allerdings oftmals zu Lasten der eigenen personenbezogenen Daten die dadurch verarbeitet werden oftmals auch so das der Betroffene gar nicht weiß was mit den Daten passiert. Personenbezogene Daten sind in der heutigen Zeit schnell und überall verfügbar. Sie sind die Währung von vielen Online-diensten. Datenschutz ist für den Betroffenen, also für jede einzelne natürliche Personen und dient dem Schutz seiner Daten, damit diese nicht veräußert oder unrechtmässig zum Beispiel im Bereich des Marketing verarbeitet werden. Sicherlich sind auch Sie nicht davon begeistert einen neuen größeren Briefkasten kaufen zu müssen nur weil der Anteil an Werbung plötzlich stark zugenommen hat. Auch sind Sie sicherlich nicht davon begeistert wenn eines Tages die Polizei vor Ihrer Türe steht um Sie zu verhaften weil Ihre personenbezogenen Daten Teil von polizeilichen Ermittlungen geworden sind.

Bedenken Sie, Sicherheit geht immer zu Lasten von Bequemlichkeit. Doch Sicherheit geht immer zu Gunsten von Ihrer persönlichen Freiheit und Kontrolle.



Das Labyrinth des Datenschutzes mit all seinen Barrieren meistern.

nen herbei zuführen die ihn in die Haftung bringen. Somit berichtet er ausschließlich der höchsten hierarchischen Ebene eines Unternehmens, was in aller Regel die Geschäftsführung selbst ist.

Alle Informationen zu denen er Zugang erhält behandelt er vertraulich. Er ist Ansprechpartner für Mitarbeiter des Unternehmens, die ihm einen Verstoß melden möchten und persönliche Fragen haben Inhalte persönlicher Gespräche mit Mitarbeitern eines Unternehmens werden und dürfen nicht mit der Geschäftsführung besprochen werden. Hier gilt ebenfalls höchste Verschwiegenheitspflicht. In sofern kann jeder Mitarbeiter ganz beruhigt mit seinen Fragen, Ängsten und Sorgen betreffend seiner personenbezogenen Daten auf ihn zu gehen.

Zu der Erfüllung seiner Aufgaben gelten natürlich Fristen und Regeln einzuhalten, die seitens der DSGVO und in Ergänzung mit dem BDSG-Neu einzuhalten sind. Insbesondere bei Verstößen muss hier rasch gehandelt werden da die Zeitspanne der Frist nach Kenntniserlangung von nur kurzer Dauer ist.

Jedem Unternehmen ist damit geholfen einen internen oder externen Datenschutzbeauftragten zu ernennen der diese wichtigen Aufgaben rundum den Datenschutz zu Minimierung des unternehmerischen Risikos von Bußgeldern übernimmt.

All diese Themen werden immer wichtiger für Unternehmen, Mitarbeiter und Privatpersonen gleichermaßen.



Mozilla Thunderbird

Thunderbird kommt mit integrierter PGP-Verschlüsselung

Nachdem sich der Sturm hinsichtlich der Key-Server der PGP-Community gelegt hat und die Verifizierung von Schlüsseln wieder erfolgreich ohne Einschränkungen vorgenommen werden kann, offenbart Mozilla eine eigenständige integrierte PGP-Lösung innerhalb ihres kostenfreien Email-Clients „Thunderbird“.

Laut einem Artikel vom 08.10.2019 bei Heise Online wird Mozilla Mitte bis Ende des Jahres 2020 mit der Version 78, so konkret wurde es hier schon benannt, ihren Email-Client die PGP-Verschlüsselung bei gebracht haben. Viele und wichtige Fragen bleiben bis jetzt allerdings noch offen und ungeklärt wie zum Beispiel die Frage wie die eigene Schlüsselverwaltung aussieht und welches Konzept sich das Unternehmen hierfür überlegt.

Eine weitere Frage wird sein, in wie weit der Endverbraucher hier technisches Wissen zur Einrichtung eines eigenen PGP-Schlüssels brauchen oder ob er mittels gut durchdachten und leicht verständlichen Assistenten durch die Einführung geführt wird.

Das Plug-In welches zur Zeit von Mozilla für die PGP-Verschlüsselung heran gezogen wird und auf den Namen „EnigMail“ hört, wird spätestens Ende kommenden Jahres eingestampft und auch nicht mehr mit Sicherheitsupdates versorgt werden. In Punkto Datensicherheit und Datenschutz geht Mozilla als

Was ist ..? Vertrauen-by-Design

In Bezug auf die Entwicklung der Künstlichen Intelligenz (KI) in fortschreitender Technik ist damit gemeint, der künstlichen Intelligenz in ihrer Entscheidungsfindung zu vertrauen. Das sagt zumindest die Wettbewerbskommissarin Frau Margarethe Vestager, die diesen Begriff erstmalig formulierte.

Dies dürfte ein zurecht wagemutiges Abenteuer werden und wirft natürlich die Frage auf nach welchen Maßgaben sich die KI zukünftig richten soll. Wer definiert die Richtlinien und ist auszuschließen das ein Multikonzern sich dieses nicht zum eigenen Vorteil zu eigen macht?



FBI—Federal Bureau of Investigation

Menschliche Neugier oder schon Überwachung?

In den USA haben FBI Agenten gegen den vierten Zusatzartikel der Amerikanischen Verfassung verstoßen in dem sie ihre beruflichen Fähigkeiten für private Suchanfragen ausnutzten.

Zehntausendfach so ein Heise Online Artikel vom 10.10.2019 wurden von den FBI Agenten Suchanfragen über Familie, Freunde, Verwandte und Bekannte ausgeführt.

Diese Neugier ist eine typisch menschliche Eigenschaft und zeigt einmal mehr worin die Schwachstelle in unserer Gesellschaft begründet ist. Doch lässt sich das einfach abschalten?

Der Grad zwischen einmaliger Suche und systematischer automatisierter Überwachung von Personen ist unheimlich schmal.

Menschen die Zugang zu so hochsensiblen Techniken haben müssen natürlich einerseits sensibilisiert und Willensstark sein. Andererseits aber auch hart sanktioniert werden, wenn Sie Ihre Macht missbrauchen.



Datenschutz-Grundverordnung

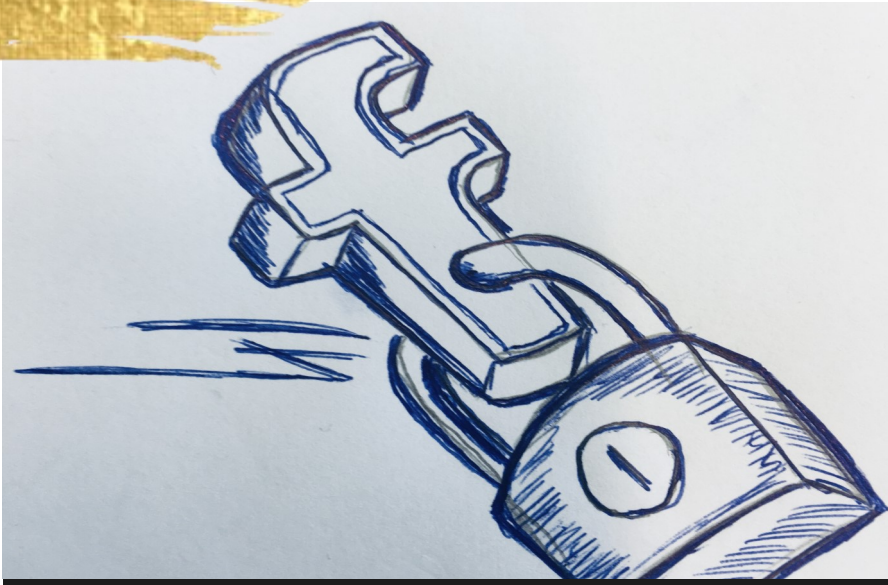
erster einen Schritt in die richtige Richtung, was durchaus hoffen lässt.

Zu wünschen bleibt, das andere Anbieter wie zum Beispiel Microsoft mit seinem Produkt „Outlook“ nachzieht und auch hier für eine integrierte PGP-Lösung sorgt. Damit wir morgen schon alle sicher, von Dritten ungelesen und unverändert unsere Emails versenden können.

Nun müssen wir uns noch bis Mitte nächsten Jahres gedulden. Natürlich kann da noch vieles passieren, was dem Projekt nicht unbedingt das Genick brechen wird, den Fortschritt allerdings verzögern kann.

Denn die Weltgrößten Regierungen haben kein Interesse daran Emails nicht mehr auslesen zu können. Natürlich alles unter dem Deckmantel der Prävention gegen Terror, Kriminalität und der allgemeinen Verbrechensbekämpfung.

Nach wie vor gilt PGP als eines der sichersten Verschlüsselungsverfahren weltweit. Die Bedienung, Erstellung und Verwaltung von Schlüsseln war bislang allerdings äußerst kompliziert, sodaß selbst IT Fachleute ihre Mühen damit hatten. Inzwischen wird die Bedienung und Nutzung immer einfacher und kundenfreundlicher was hoffentlich dafür sorgt, das mehr Privatpersonen diese Technologie der Verschlüsselung von Daten mehr nutzen werden bis es in den Alltag vollständig integriert ist.



Facebook

Facebook: Einführung von Datenverschlüsselung

Wenn man am tiefsten Punkt angelangt ist, kann man sich erhobenen Hauptes in entgegengesetzter Richtung wieder Auftrieb verschaffen in dem man dann schließlich doch das tut was von einem gefordert wird.

So könnte man die aktuelle Richtung des Unternehmens Facebook treffend beschreiben. Denn nach all den Datenschutz-Verstößen und Unmengen von verhängten Bußgeldern als auch hämender Kritik, geht Facebook in die Offensive und will die grundsätzliche Verschlüsselung von Daten nicht nur in den Messangern und Chats sondern direkt im System selbst integrieren und weiter ausbauen. Das geht aus Artikeln von „Die Zeit“ als auch der „Tagesschau“ vom 04.10.2019 hervor.

Ohne Zweifel ist das zu befürwortender Schritt. Doch bleibt von der Bitternis der Vergangenheit ein fahler Beigeschmack. Kann man Facebook zukünftig mehr Vertrauen schenken und darauf vertrauen das das Unternehmen sorgsam mit personenbezogenen Daten umgeht? Diese Frage wollen wir mit gebotener Skepsis im Raume stehen lassen, warten und darauf vertrauen das Mark Zuckerberg nun doch endlich Wort hält.

Was ist ..? Privacy-by-Design

Dieser Begriff ist einer der ältesten im Bereich des Datenschutzes und beschreibt das der Datenschutz schon durch die Technik selbst und vor Erhebung einzuhalten ist.

Mit anderen Worten gelten hier alle technischen und organisatorischen Maßnahmen die erfüllt sein müssen um den Schutz der Daten als auch deren Sicherheit zu gewährleisten.



Visitenkarten

Der Mythos ... Visitenkarte

Die Übereignung von Visitenkarten ist eines der Negativ-Sinnlosen-Beispiele im Sinne der DSGVO.

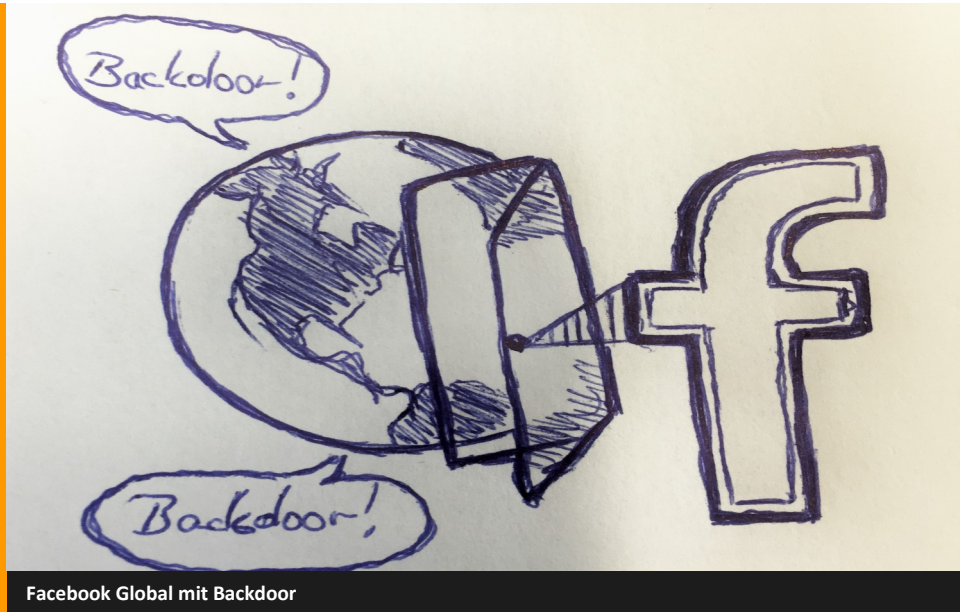
Denn demnach muss derjenige der die Visitenkarte übergibt eine Einwilligungserklärung zur elektronischen Verarbeitung der Kontaktdaten unterschreiben und auf die Verarbeitungsmöglichkeiten informiert werden.

Der Aufwand ist enorm hoch und absolut nicht umsetzbar.

Im Grunde entsteht bereits eine Einwilligung in dem Moment in dem die Visitenkarte übergeben wird. Die Daten werden gespeichert auf dem Papier/Pappe bereits übergeben. Und der Zweck der Übergabe ist die Erreichbarkeit zu ermöglichen und zu dokumentieren.

In sofern eine eindeutige Angelegenheit. „Mit gesundem Menschenverstand denken und Handeln.“ ist die Devise und nicht alles auf die Goldwaage legen bzw. tot bürokratisieren.

Sollte es in dieser Angelegenheit Klagen geben, was ich mir nicht vorstellen kann, so werden die Gerichte hierzu eine Entscheidung treffen müssen.



Natürlich stößt das bei den Regierungen insbesondere der USA selbst als auch Großbritannien und Australien die als erste benannt werden nicht gerade auf großen Zuspruch. Denn Sie alle wollen das Facebook eine Hintertür einbaut, damit Regierungen zum Schutze der Kinder als auch zum Zwecke der allgemeinen Verbrechensbekämpfung dennoch Einsicht nehmen können. Nimmt mal allein diese Argumentation, so könnte man das als gut und richtig erachten, wenn man nicht wüste das die Regierungen weit mehr tun wenn sie die Gelegenheit bekämen.

Nun, dann brauchen wir eine Verschlüsselung gar nicht erst einführen, sollte Facebook dem auch nur im Ansatz nachkommen. Denn die Verschlüsselung von Daten soll ja gerade das unterbinden.

Noch ist das alles Zukunftsmusik, Facebook hat jedoch zugesichert, mit den Behörden zu sprechen und Mechanismen zu entwickeln, die die Verschlüsselung vorantreibt und im Vorfeld zu übermittelnde Daten wie zum Beispiel Bilder und Fotos beim Versender auf Illegalität prüft. Wie das funktionieren soll ist noch nicht klar. Doch das würde schon jetzt bedeuten, das Facebook im Hintergrund agiert und weiterhin Geräte und Profil ausspioniert.

Wollen wir mal mit einer gehörigen und gesunden Portion Skepsis allerdings auch mit einem Gefühl des Wohlwollens den weiteren Verlauf beobachten.



Facebook

Bußgelder in Deutschland bei Datenschutz-Verstößen

Seit Einführung der europäischen Datenschutz-Grundverordnung (DSGVO) und für Deutschland als nationale Ergänzung das Bundesdatenschutzgesetzes-Neu (BDSG-Neu), hagelt es regelrecht euweit Bußgelder in Millionenhöhe. Allen voran ist das Unternehmen Facebook mit seinen zahllosen Verstößen führend sowohl in der Kritik, in ihren Skandalen was Datenschutz-Verstöße als auch die Höhe der bisher verhängten Bußgelder angeht.

Am 25.06.2019 haben die unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) ein Modell zur Berechnung von Bußgeldern erarbeitet. Dieses Dokument ist bis heute nicht veröffentlicht worden und wird es auch in absehbarer Zeit nicht. Begründet wird das mit der Unsicherheit, das Unternehmen Ihre Verstöße daran angleichen um möglichst wenig an Ihren Prozessen zu ändern und im Zweifelsfall mit relativ geringen Strafen davon zu kommen sofern eine Prüfung vollzogen wurde.

Dieser Berechnungsentwurf stieß bei der Taskforce Findings des Europäischen Datenschutzes (EDSA) auf gesteigertes Interesse. Denn im Gegensatz zu anderen Modellen liegt diesem eine systematische, transparente und nachvollziehbare Bemessung zu Grun-

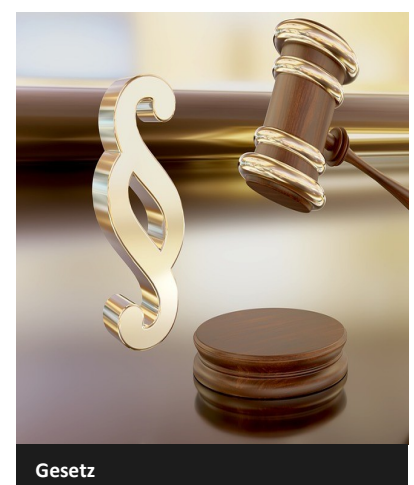
Was ist ..? Trust-by-Design

Ist ein weiterer Begriff der in Bezug auf den Datenschutz immer wieder vorkommt. Gemeint ist damit das was Frau Margarethe Vestager mit „Vertrauen-by-Design“ in halbwegs deutschen Worten meint.

Es meint dem Stand der Technik und seiner Dienste zu vertrauen.

Nun das fällt sicherlich nicht nur mir schwer sondern vielen Menschen. Denn irgend jemand, irgend ein Konzern wird sowohl die Technik als auch die dahinterliegenden Dienste erschaffen haben.

Ganz sicher verfolgt man dann nicht dem Grundsatz „Zum Wohle der Allgemeinheit“. Sondern wie die Geschichte uns lehrt „Zum Wohle des eigenen Selbst“.



Gesetz

EuGH § Cookies

Nach einem jüngsten Entscheid des EuGH's bedarf das setzen und ablegen eines Cookies ohne technische Relevanz der aktiven Einwilligung durch den Besucher einer Webseite. D

amit sind insbesondere Cookies zu Werbe- und Analysezwecken gemeint.

Die Einwilligung darf nicht vorausgefüllt durch den Webseitenbetreiber sein. Auch dürfen die Texte nicht so verfasst werden das ein nicht-aktives Handeln durch den Webseitenbesucher gleichzusetzen ist mit einer Einwilligungserklärung.

Der Betreiber einer Webseite ist aufgefordert, seiner Informationspflicht in leicht verständlichen Worten in Bezug auf zu setzende Cookies nach zukommen.



Bußgelder und Macht

de um entsprechende Bußgelder bei Datenschutz-Verstößen verhängen zu können.

Der Bundesdatenschutzbeauftragte Herr Ulrich Kelber äußerte sich dazu, in dem er die bisherige Zurückhaltung Deutschlands bei der Erhebung von Bußgeldern mit abnehmender Tendenz und somit auch in Deutschland Bußgelder in Höhe von Millionenhöhe sehe.

Am 18.10.2019 wird darüber entschieden wie das Bußgeldkonzept zur Berechnung von Bußgeldern zukünftig ausgestaltet sein wird. Nur eines ist bis dato sicher, die Höhe der Bußgelder bei Datenschutz-Verstößen wird auch in Deutschland steigen.





Staatliche Unentschlossenheit

Zwischen bürokratischer Starrsinnigkeit und Datensicherheit

In der Regierung oder zumindest in der IT technischen Administration scheint man der Auffassung zu sein, dass Datenschutz und Datensicherheit keine besonders hohe Bedeutung hat.

Denn wie sollte es anders zu erklären sein, wenn auf Anfrage von Abgeordneten unterschiedlicher Parteien der Wunsch und die Bitte geäußert wird, einen als sicher geltenden Messenger-Dienst zu installieren und dies abgeschmettert wird.

Die Begründung ist in gewisser Weise nachvollziehbar, denn es heißt aus dem zuständigen IT Ressort, dass es sich um keine Standard-Applikation handelt und diese erst getestet werden muss. Soweit typisch deutsch und bürokratisch, aber nachvollziehbar und in Ordnung.

Doch statt das man genau das tut, die Software zu testen und ausgiebig auf Sicherheit zu prüfen, wird abgewiegelt und schlimmer noch eine Empfehlung zur Nutzung eines mehr als fragwürdigen Messengers zu zugehen.

Worum geht es im Detail? Nun, der Wunsch bestand darin, den

Was ist ..?

E-Privacy

Hier handelt es sich um eine Verordnung, die aus dem Jahre 2002 stammt.

Ihr Ziel ist die Stärkung des Datenschutzes in aktuellen Kommunikationsmedien. Konkret, wer darf welche digitalen Spuren des Einzelnen verfolgen und für sein Geschäftsmodell verarbeiten.

Die enthaltenen Punkte der Betrachtung sind:

- Keine Datenverarbeitung ohne Einwilligung
- Einfacher Schutz vor Online Tracking
- Privacy-by-Default
- Grenzen für offline Tracking
- Recht auf Verschlüsselung
- Transparenz von staatlichen Übergriffen

Diese Verordnung ist noch sehr weit davon entfernt verabschiedet zu werden. Denn die Lobbyisten der Werbe- und Trackingfirmen wehren sich mit eiserner Hand und sehen durch diese Verordnung ihre Geschäftsfelder in Gefahr.

Ob, wann und in welcher Form es zu einer konkretisierten Entscheidung kommt, bleibt abzuwarten.



Entscheidungsfindung

Die Nutzung von Dash-Cams

Der Straßenverkehr nicht nur in den Städten und Dörfern sondern vor allem auf den Autobahnen und Landstraßen lässt eine gewisser Verrohung nicht vermissen.

Um dem entgegen zu wirken erfreuen sich sogenannte Dash-Cams die in den Fahrzeugen verbaut und mit je einer Kamera für vorne und hinten ausgestattet sind, immer größerer Beliebtheit.

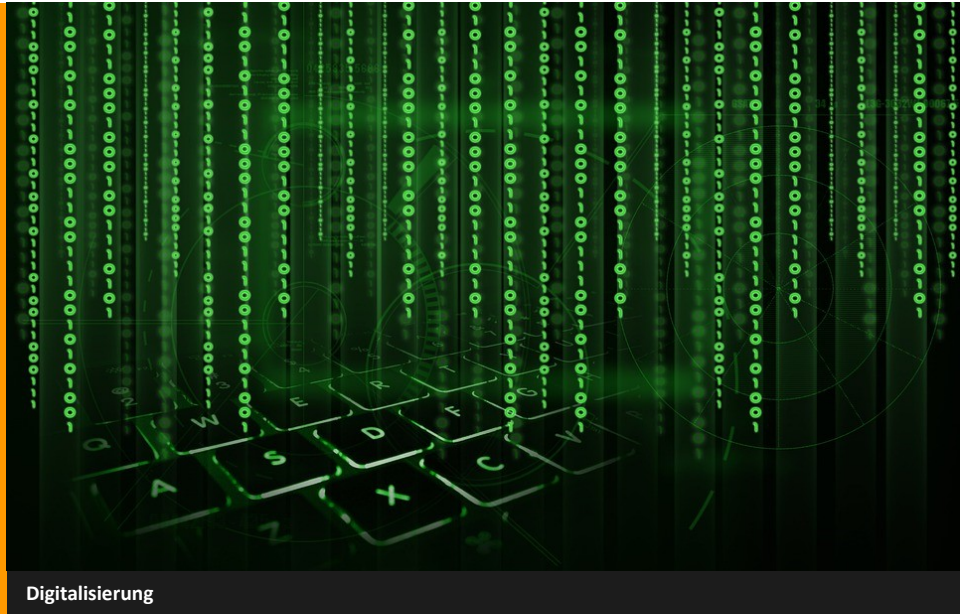
Nun ist aber gerade die permanente Aufzeichnung von personenbezogenen Daten ohne Einwilligung des Beobachteten, und Nummernschilder sind genau solche nicht mit den Richtlinien der DSGVO vereinbaren.

Die richterlichen Richtlinien zur Nutzung von Dash-Cams sind:

- Kurze und zweckbezogene Aufzeichnungen
- Überschreibungen nach kurzer Zeit.

Somit wird hier ein Kompromiss geschaffen. Inzwischen gibt es bei den Kfz-Versicherungen Vergünstigung bei Nutzung.

Zudem haben Dash-Cams eine abschreckende Wirkung.



Digitalisierung

Messenger „Signal“ zu verwenden der als sicher gilt und auch von namenhaften Whistleblowern wie Edward Snowden verwendet wird. Stattdessen wird auf die von Facebook aufgekauften WhatsApp Dienste verwiesen und direkt empfohlen.

Wenn ich mir überlege das es im Parlament nicht gerade um die Klärung von Mittagessen oder andere belanglose Informationen geht, sondern vielmehr um inhaltlich brisante und sensible Inhalte, dann ist das nicht nur im höchsten Maß fragwürdig sondern grobfahrlässig.

Gerade in Regierungsangelegenheiten sollten doch die möglichst höchsten Sicherheitsvorkehrungen getroffen werden. In gewisser Hinsicht hat die Regierung seinem Volk gegenüber eine Vorbildfunktion der sie in keinsten Weise nachkommt.

Denn wie soll man Privatpersonen und Endverbraucher davon überzeugen mehr auf ihre eigenen personenbezogenen Daten Acht zu geben wenn selbst die Regierung es aus Gründen der Bequemlichkeit in Kombination von starrer Bürokratie nicht schafft.

Datenschutz und Datensicherheit geht anders. Uns bleibt nur die Hoffnung das sich die IT unseres geschätzten Parlamentes eines Besseren besinnt und weise handeln wird.



Staatstrojaner-Hersteller in der Kritik wehren sich

Es gibt mehrere Firmen deren Aufgabe darin besteht Programme zu Spionagezwecken zu entwickeln. Nachbekanntwerden der Software als auch der jeweiligen Anbieter die natürlich in Kritik geraten sind. Fangen die nun an sich zu wehren.

Das die Herstellung von Schnüffelsoftware zwar spannend, jedoch fraglich ist dürfte unstrittig sein. Wenn Regierungen allerdings derartige Produkte kaufen, anpassen und auf die Bevölkerung gleich welchen Landes loslassen, ist das ein Akt des Vertrauensmissbrauchs gegenüber dem Volk als auch ein Akt staatlicher systematischer Überwachung.

Natürlich sind die Hersteller dieser Spionageprogramme nicht daran interessiert in den Fokus der Öffentlichkeit und schon gar nicht von kritischen Medien zu geraten. Netzpolitik.org eine der Plattformen die sich sehr intensiv um Datenschutz und Datensicherheit bemühen haben mehrfach sachlich jedoch kritisch und durchaus hinterfragend mit dem Hersteller und seiner Anwendung auseinander gesetzt und emsig darüber berichtet.

Was ist ..?

Der Cloud-Act

"Cloud Act" steht für "Clarifying Lawful Overseas Use of Data Act" und beschreibt ein US amerikanisches Gesetz welches am 23. März 2018 unter der Regierung Donald Trumps als amerikanischer Präsident unterzeichnet wurde und den Datenzugriff von US Firmen und Konzernen regelt.

Konkret geht es darum das US Behörden uneingeschränkten Zugriff auf Daten aller Art, nicht nur Geschäftsdokumentationen sondern auch auf personenbezogene Daten von US Firmen, Firmen die in den USA einen Sitz haben, als auch Firmen die mit US Firmen kooperieren haben sollen. Dabei spielt es keine Rolle wo und in welcher Form die Daten vorliegen.

Somit ist das Gesetz der "Cloud Act" das direkte Gegenteil der DSGVO.



Wer braucht einen Datenschutzbeauftragten?

Gemäß Artikel 37 der Datenschutzgrundverordnung ist jedes Unternehmen angehalten einen Datenschutzbeauftragten zu benennen in dem automatisiert personenbezogene Daten verarbeitet werden.

Unabhängig von der Zahl der Mitarbeiter die permanent mit personenbezogenen Daten arbeiten ist in jedem Unternehmen der Datenschutz dieser personenbezogenen Daten sicherzustellen.

Aktuell gilt ab einer Mitarbeiterzahl von 20 die permanent mit personenbezogenen Daten arbeiten ist ein interner oder externer Datenschutzbeauftragter zu benennen.

Das heißt allerdings das man bei geringerer Anzahl an Mitarbeitern den Datenschutz vernachlässigen darf oder gar nicht erst dafür sorgen muss.



Nun, da der Anbieter immer größeren Bekanntheitsgrad erlangt und klar wird, das nicht nur Deutschland sondern auch andere Länder wie die Türkei und im arabischen Raum von dem Anbieter beliefert wird, können diese eben nicht mehr im geheimen Untergrund wirken.

Es handelt sich um ein Unternehmen Namens FinFisher über die in inzwischen 84 Artikeln bei Netzpolitik.org berichtet wurde. Eine Aufstellung dieser Artikel ist bei Netzpolitik.org einzusehen (<https://netzpolitik.org/tag/finfisher/>)

Nun geht FinFisher rechtsanwaltlich gegen Netzpolitik.org vor in dem Versuch weitere Berichtserstattung zu unterbinden und die Stimme der Vernunft zum Schweigen zu bringen. Dies bezeichnet einen direkten Angriff auf unsere Demokratie, Presse- und Meinungsfreiheit. Zumal man von einer Meinung kaum reden kann, wenn Fakten für sich selbst sprechen.

Netzpolitik.org braucht Unterstützung. So ihr Aufruf auf der eigenen Webseite. Und ja, die sind in jeder Hinsicht unterstützenswert. Wir werden den weiteren Verlauf mit Spannung und leicht zitterigen Beinen verfolgen.

Das Statement von Netzpolitik.org ist eindeutig: „Wir lassen uns nicht von der Überwachungsindustrie einschüchtern.“.



Tool: Datenverschlüsselung mit Vera Crypt

Tools für mehr Sicherheit

Heute: Vera Crypt

Das Programm VeraCrypt ist der Nachfolger des inzwischen gehackten und somit als unsicher geltenden TrueCrypts. Bisher wird seitens des BSI VeraCrypt eine Sicherheit der Datenverschlüsselung bescheinigt.

Mit beiden Programmen ist es möglich einen verschlüsselten Datencontainer zu erstellen und auch vollständige Festplatten zu verschlüsseln. Der Hersteller IDRIX ist in Frankreich/Paris ansässig. Die Software ist ein Open Source Projekt was bedeutet das der Quellcode des Programms für alle offen einsehbar ist. Genau das ist neben der gebotenen Sicherheit durch den Einsatz unterschiedlicher Algorithmen ein Argument des Vertrauens, da hier kein Staat und keine Regierung im Hintergrund mitwirkt um Backdoors einzubauen.

Die Bedienung und Einrichtung von Datenträgern ist recht einfach gehalten. Der integrierte Assistent unterstützt dabei sehr gut. Zur Anwendungen der Verschlüsselung kommen Algorithmen wie AES, Twofish, Camellia und Serpent die ihre gemeinsame Stärke durch aktives Zusammenspiel entfalten.

Was ist ..?

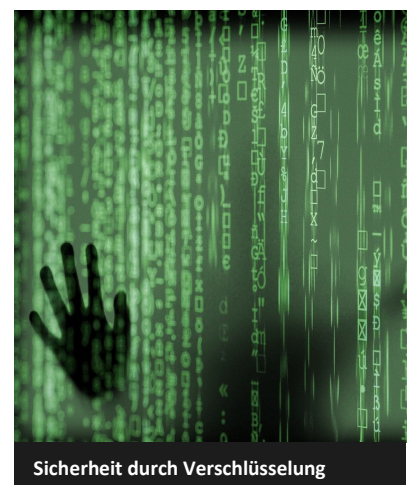
Das Bundesdatenschutzgesetz-Neu

Das Bundesdatenschutzgesetz (Neu) beinhaltet die nationale Gesetzmäßigkeit und ist als Ergänzung zur Datenschutzgrundverordnung zu verstehen.

Jedes Land der EU hat die Möglichkeit ein solches Nationalgesetzbuch als Ergänzung zur DSGVO zu betreiben.

Das Bundesdatenschutzgesetz (Neu), zusammen mit der DSGVO ist am 25.05.2018 in Kraft getreten ist somit der DSGVO untergeordnet.

Das alte Bundesdatenschutzgesetz wurde mit Einführung des Neuen vollständig abgelöst.



Sicherheit durch Verschlüsselung

Themen der nächsten Ausgabe

- Aufsichtsbehörden: Globaler Standard
- Project JEDI: Die Pentagon-Cloud
- Unterstützung des Datenschutzbeauftragten
- Implantate-Register-Errichtungsgesetz
- Überwachung in Deutschland durch Arbeitgeber

Weitere Themen können folgen. Änderungen werden vorbehalten.



Abgeschlossen und Verschlüsselt

Natürlich kann und wird es niemals eine hundertprozentige Sicherheit geben, denn ist und bleibt ein stetiger Wettstreit des Technischen Fortschrittes, findiger Entwickler, Hacker und der Zeit.

Was bleibt ist den eigenen persönlichen Schutz weitestgehend auszubauen und es Angreifern dabei so schwer als möglich zu machen die eigenen persönlichen Daten zu erlangen und zu manipulieren.

VeraCrypt ist kostenfrei auf der Herstellerseite zum Download angeboten und bedeutet gerade für Privatpersonen einen ersten guten Schritt um sorgsam mit seinen Daten umzugehen.

Das Programm ist neben unterschiedlichen Versionen auch als sogenannte Portable App verfügbar. Was soviel bedeutet das diese nicht ins Betriebssystem installiert wird und das laufende System somit nicht belastet.

Es ist dazu prädestiniert auf einem mobilen Datenträger Anwendung zu finden um stets sichere Daten mit sich zu führen. Denn selbst wenn ein solcher USB-Stick mal verloren geht, kann der Finder mit dem Inhalt nichts anfangen.

Wer einen Hardware Schlüssel wie zum Beispiel einen YubiKey verwendet, der wird eine entsprechende Unterstützung dessen innerhalb von VeraCrypt für noch mehr Sicherheit finden.



Wichtige Termine

Die folgenden Termine wollen beachtet werden:

Sommer 2020	Thunderbird V.78 mit PG
Herbst 2020	Ende des Supports von EnigMail.
18.10.2019	Abstimmung des Bußgeld-Konzeptes

Der Datenschutz-Witz

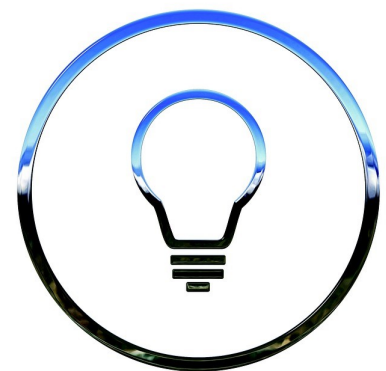
Ein Geschäftsführer ist wegen der DSGVO verzweifelt. Er ruft einen befreundeten Geschäftsführer an und fragt: „Kennst du einen guten Datenschutz-Berater?“. Dieser antwortet mit :“Ja“. „Kannst du mir mal seine Nummer geben?“. „Nein.“

Was ist ..? Ein Kryptotrojaner

Oder auch gern Ransomware genannt ist eine erpresserische Schädlingssoftware.

Auf dem Kundenrechner eingetroffen und ausgeführt, oftmals durch unachtsames Doppelklicken von Emailanhängen und ausgeprägter Neugier des Lesers verschlüsselt die Software sämtliche Dateien des Systems und macht für den eigentlichen Eigentümer unbrauchbar.

In der Regel taucht dann eine Nachricht auf die mit einer Geldforderung für den Austausch des Entschlüsselungscodes seine Aufmerksamkeit macht.



Ideen und Erinnerungen



Impressum

Alle hier erschienen Artikel, Fotos und Grafiken wurden durch uns selbst hergestellt bzw. stammen von Partnern von denen wir entsprechende Lizenzvereinbarungen haben.

Einige Grafiken kommen unter anderem vom Anbieter Pixabay.com.

Für Inhalte fremder Webseiten und den hier veröffentlichten Links tragen wir keine rechtliche Verantwortung. Diese dienen lediglich der Quellenangabe unserer Informationen und zum nachlesen interessierter Leserinnen und Leser für nähere Details.

Herausgeber ist allein:

Ihr externer Datenschutzbeauftragter Gehrman

In Person:

Herr Markus Don Alfred Gehrman

Email:

datenschutz@mdagehrmann.de

WWW

<https://datenschutz.mdagehrmann.de>



Links und URL's

Links

Die nachfolgenden Links sind Basis der hier erschienen eigenen zusammengefassten Artikel. Für den Inhalt der verlinkten Seiten übernehmen wir keinerlei rechtliche Verantwortung.

Thunderbird und PGP

<https://www.heise.de/security/meldung/Thunderbird-integriert-Email-Verschluesselung-mit-OpenPGP-4549027.html>

Facebook und Verschlüsselung

<https://www.zeit.de/digital/datenschutz/2019-10/facebook-behoerden-zugang-verschluesselung-nachrichten>

<https://www.tagesschau.de/ausland/facebook-verschluesselung-101.html>

Bußgelder von Datenschutz-Verstößen in Deutschland

<https://www.datenschutzbeauftragter-info.de/dsk-modell-zur-berechnung-von-dsgvo-bussgeldern/>

EuGH: Cookies

<https://www.datenschutzbeauftragter-info.de/eugh-aktive-einwilligung-fuer-cookies-erforderlich/>

Netzpolitik.org

<https://netzpolitik.org/tag/finfisher/>





Unser Bestreben und unser Ziel

Datenschutz und Datensicherheit sind zwei Begriffe in unserer Gesellschaft die an Bedeutung seit dem 25.03.2018 stark zugenommen haben. Denn mit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) auf EU-Ebene wurden die Rechte des Einzelnen und seiner Person verbessert.

Die Freiheit und der Wohlstand in dem wir in Deutschland leben ist nicht selbstverständlich, war es und wird es niemals sein.

In unserer Vergangenheit gab es Menschen die sich für die heutigen Rechte eingesetzt haben. Nicht wenige von Ihnen verloren dabei ihr Leben. Auch heute gibt es eine Vielzahl an Menschen die dem Ruf der Freiheit folgen. Sich für aufopfern mit dem Bestreben die Welt ein bisschen besser für alle zu machen. Denn der Schutz unserer Daten, gleich welcher Art sollte uns alle wichtig sein.

Wir tragen Verantwortung nicht nur für uns selbst. Sondern für jene und Handeln, Ihr Engagement die vor uns waren, als auch für jene die nach uns folgen werden.

In sofern darf es niemals und zu keiner Zeit möglich sein das wir es zulassen das andere mit unseren Daten ohne unser Wissen und unsere Einwilligung Handel treiben oder sie gar zweckendfremd für gesetzeswidrige Dinge missbrauchen.

Es ist unsere menschliche Pflicht alles dafür zu tun es den weltweiten Geheimdiensten und auch jenen mit kriminellen Energien so schwer als möglich zu machen uns in unserer Persönlichkeit zu missbrauchen.

Der gläserne Mensch muss zu einer aussterbenden Rasse werden und kein allgemeines Handelsgut sein.

So erreichen Sie uns

Falls Sie weitere Informationen zu unseren Dienstleistungen und Produkten benötigen, kontaktieren Sie uns:

Ihr externer Datenschutzbeauftragter Gehrmann

Email:
datenschutz@mdagehrmann.de

WWW
<https://datenschutz.mdagehrmann.de>