Datenschutz DSGVO/BDSG –neu/…

kurz und knapp

Was das mit uns zu tun hat

Um was es dabei überhaupt geht

Wie man sinnvoll damit umgeht

Vorneweg

Personenbezogene Daten

Datenschutz

versus

Vertraulichkeit,
Integrität,
Verfügbarkeit

Datensicherheit

Verantwortlich ist immer der …

Geschäftsführer

und jeder,

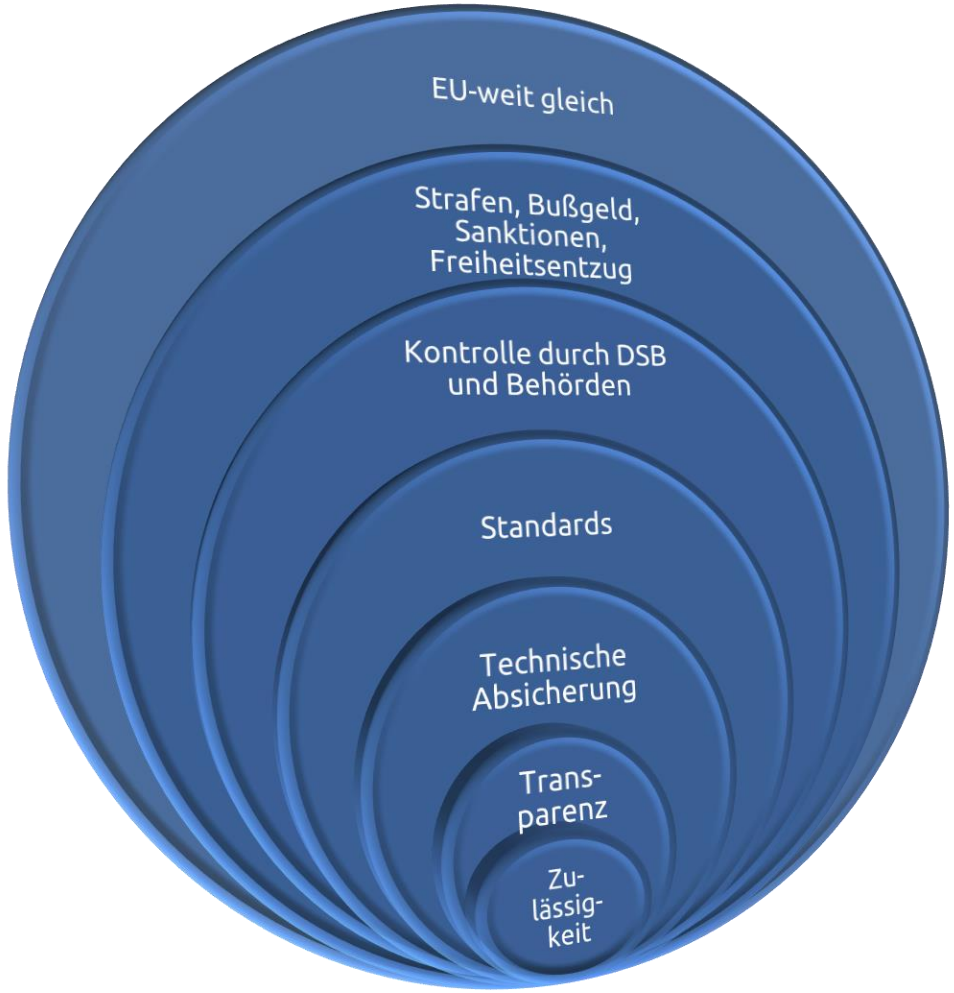
der mit personenbezogenen Daten umgeht

Wer haftet?

- Das Unternehmen (GmbH, AG, Verein, …)
  - Begründung: Direkt so in DSGVO geregelt
- Unter Umständen jeweiliger Geschäftsführer persönlich
  - Begründung: Organisationsverschulden nach §130 OWiG
- Der Mitarbeiter, der den Datenverstoß begeht.
  - Begründung: Er ist nach OWiG der Täter!

Quellenhinweis Ordnungswidrigskeitengesetz: https://dejure.org/gesetze/OWiG

DSGVO - Was es ist



Die EU Datenschutz-Grundverordnung 2016/679 (EU General Data Protection Regulation) …

- ist ein einheitliches EU Gesetz das für Unternehmen innerhalb der EU gilt und für Auftragsdatenverarbeiter dieser weltweit.
- ist mit schmerzhaften Sanktionen verbunden.
- wird scharf geschaltet am 25. Mai 2018
- bietet erhebliche Möglichkeiten den eigenen Datenschutz erheblich zu verbessern

Erklär-Video vom BvD e.V.

Verbindlich für Unternehmen, …

- die ihren Sitz in der EU haben
- in der EU Daten verarbeiten
- Waren in die EU verkaufen
- zwar außereuropäisch sind,
  - aber in einer Niederlassung innerhalb der EU Daten verarbeiten (Zuständigkeit nur für EU-Niederlassung)
  - die für europäische Unternehmen Daten verarbeiten
  - Aber Waren oder Dienstleistungen für Einzelpersonen anbietet oder das Verhalten einzelner kontrolliert

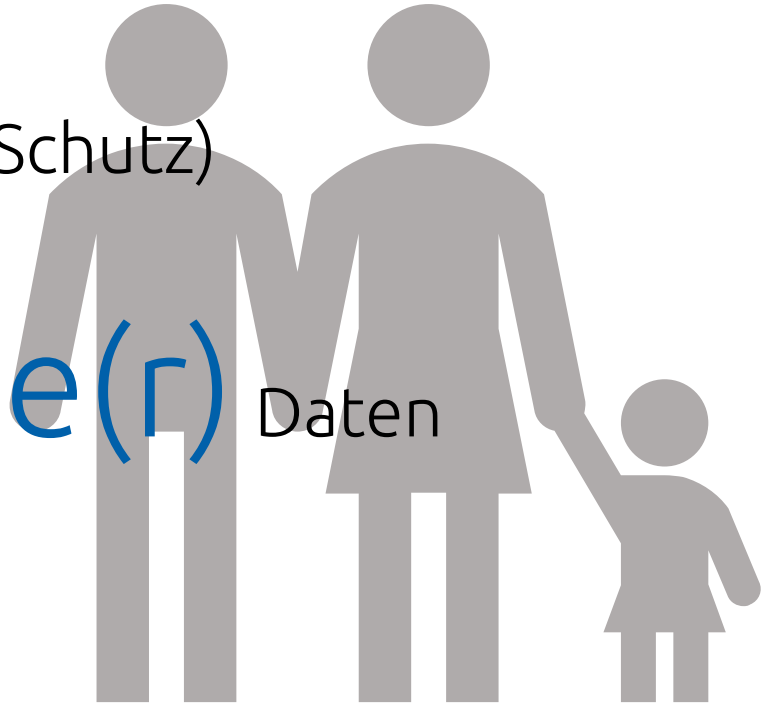
Zielsetzung und Auswirkungen

- Erstellt für die Bürger der EU, damit sie mehr Kontrolle ihrer personenbezogener Daten bekommen.
- Unternehmen und Organisationen müssen künftig …
  - … die Daten der EU Bürger müssen durchgängig geschützt werden
  - … Verstöße innerhalb von 72 Stunden gemeldet werden
  - …. in Lösch-/Änderungsrecht umgesetzen
  - … auf Datensparsamkeit geachtet werden
  - … mit Strafen bis €20M oder 4% des weltweiten Umsatzes rechnen

Ziel

Es geht immer um (den Schutz)

personenbezogene(r) Daten



Damit um das Grundrecht der informationellen Selbstbestimmung und die daraus resultierenden Pflichten der Verantwortlichen und der Auftragsdatenverarbeiter

Sie sind betroffen! Datenschutzbeauftragter?

Es sind alle europäischen Unternehmen betroffen, die personenbezogene Daten hantieren, und das sind schon Name und Vorname, also eigentlich …

alle

und deren Auftragsdatenverarbeiter weltweit. Das heißt aber nicht, das jedes Unternehmen einen Datenschutzbeauftragten benötigt.

Nicht betroffen

Es handelt sich um keine personenbezogenen Daten

Mitarbeiter

Kunden

Lieferanten

Es handelt sich um den privaten oder familiären Bereich

Besondere personenbezogene Daten

Gemäß Art. 9 DSGVO gibt es besondere Daten, die von der gewöhnlichen Verarbeitung grundsätzlich ausgeschlossen sind. Die Verarbeitung folgender Daten ist untersagt:

- Rasse und ethnische Herkunft
- politische Meinung
- Gewerkschaftszugehörigkeit
- Religiöse und weltanschauliche Überzeugungen
- Genetische und biometrische Daten einer Person
- Gesundheitsdaten
- Daten über die sexuelle Orientierung

Rechte der Betroffenen

Betroffene haben folgende Rechte

Auskunft

Löschung

Berichtigung

Widerspruch

Datenübernahme (neu!)

Accountability - Rechenschaftspflicht

- War die Verarbeitung rechtmäßig? Auf dem Grundsatz vom Treu und Glauben und leicht nachvollziehbar?
- Ist die festgelegte Zweckbindung eingehalten (feste, eindeutige, rechtmäßige Zwecke) mit dem Verbot einer Weitergabe zu nicht vereinbarten Zwecken?
- Datenminimierung durch Beschränkung auf das dem Zweck angemessene und notwendige Maß?
- Sachlich richtige/aktuelle Daten mit Maßnahmen zur Auskunft, Löschung und Berichtigung?
- Zeitliche Begrenzung der Datenhaltung, höchstens so lange, wie es für die Verarbeitungszwecke nötig ist?
- Ausreichende TOMs zum Schutz der Daten vor unbefugter/unrechtmäßiger Verarbeitung, Verlust, Zerstörung oder Schädigung?
- Sind die nötigen Prozesse definiert (z.B. Datenschutzfolgeabschätzung) und werden diese insbesondere auch der Meldeprozesse eingehalten?

Wie sollten Sie vorgehen?

- Noch ungesetzt? Dann am besten sofort starten!
- Wählen Sie sich einen kompetenten Partner,
  - der den Datenschutz und ihr Geschäft versteht
  - der rasch umsetzt und dabei gesetzlichen und geschäftlichen Nutzen kombiniert
- Starten Sie mit einer Ist-Aufnahme, bestimmen Sie den Reifegrad
- Klären Sie Ihre Risken, priorisieren Sie und setzen Sie gezielt um

Vorgehensmodell

Wo überall verarbeite ich personenbezogene Daten?	Bestandsaufnahme intern Auftragsverarbeiter inkludieren
Verarbeite und nutze ich die Daten gesetzeskonform? Auf welcher Grundlage?	Awarenessgenerierung, Anpassung von AGB, DSE, … DSB bestellen (ggfs.)
Kann ich auf alle personenbez. Daten zugreifen, diese berichtigen, löschen, Auskunft geben?	Verfahrensüberprüfung, Vertragsanpassungen, Verfahrensverzeichnis
Sind ausreichend Maßnahmen zur Daten-Sicherheit getroffen?	Tech. & organische Maßnahmen Review, Kommunikation
Wie stelle ich dauerhaft sicher, dass Vorgaben eingehalten werden und dass ich bei Verletzungen schnell informiere?	Handlungsanweisungen Prozesse definieren, kommunizieren & testen ISMS (27001 o.dgl.)

Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO)

- Es muss mindestens eine der folgenden Bedingungen erfüllt sein:
- Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Antrag der betroffenen Person erfolgen;
- die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;
- die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;
- die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.
- Quelle: Art. 6, Abs. 1 EU-DSGVO – Stand 27.04.2017, vgl. auch BDSG-neu, Teil 2

Begriffe

AV Auftragsverarbeitung
(vgl. früher ADV)

VVT Verzeichnis für Verarbeitungstätigkeiten
(vgl. früher Verarbeitungsverzeichnis)

TOM(s) Technische und organisatorische Maßnahmen

DSB
Datenschutzbeauftragter

DSFA
Datenschutzfolgeabschätzung

Meldepflicht
innerhalb 72 Stunden

Datenschutz-Folgeabschätzung

- Im Vorfeld, vor Einführung eines neuen Verfahrens oder Prozesses ist ist zu prüfen, was getan werden muss, um den Datenschutz zu gewährleisten.
- Hierzu werden dem Datenschutzbeauftragten alle relevanten Informationen zur Verfügung gestellt (siehe Verfahrensverzeichnis)

- Das heißt z.B.: Aktionen wie „Jetzt stellen wir mal von unseren Vertrieblern Fotos auf die Webseite“ können nicht per Zuruf erfolgen sondern bedürfen immer der Prüfung durch den DSB

Beispielhafte Empfehlung

TOM
Technische und organisatorische Maßnahmen

Technische & Organisatorische Maßnahmen (TOM)

DSGVO, Art. 32 fordert „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Keine weitere Konkretisierung aber folgende Schutzziele:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- Dauerhaftes Sicherstellen von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- Prozess zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs (techn. & org. Maßnahmen) zur Gewährleistung der Sicherheit der Verarbeitung.

8 Gebote des Datenschutzes (§ 64, Abs. 3, BDSG-neu)

1. Zugangskontrolle (beispielsweise Sicherung von Serverräumen mit PIN Code)
2. Datenträgerkontrolle (z.B. Sicherung von Datenträgern vor unbefugtem Lesen)
3. Speicherkontrolle (z.B. Verhinderung von Änderung personenbezogener Daten)
4. Benutzerkontrolle (z.B. Einschränkung der Anzahl von Nutzer die ein System verwenden)
5. Zugriffskontrolle (z.B. Nur eine ausgewählte Anzahl an Personen kann ein System verwenden)
6. Übertragungskontrolle (z.B. Feststellung an welcher Stelle personenbezogene Daten übertragen werden bzw. wurden)
7. Eingabekontrolle (z.B. die Dokumentation darüber, an welcher Stelle, durch wen und wann welche Daten übertragen wurden)
8. Transportkontrolle (z.B. Gewährleistung darüber, dass beim Transport von Daten die Daten geschützt sind)

Hinzu kommen folgende Punkte:

1. Wiederherstellbarkeit (sicher stellen, dass verloren gegangene/beschädigte Systeme wiederhergestellt werden können)
2. Datenintegrität (sicher stellen, dass personenbezogene Daten durch Beschädigungen nicht verändert werden können)
3. Verfügbarkeitskontrolle (sicher stellen, dass personenbezogene Daten vor Verlust geschützt sind)
4. Trennbarkeit (Gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können)

TOM – Techn. & organisatorische Maßnahmen

- Sicherheitskonzept
- Auswahlkonzept → Programme, die … Privacy by Design&Default
- Sicherungskonzept
- Berechtigungskonzept
- Löschkonzept
- Berichtigungskonzept
- Konzept zur Erfüllung von Informationsauskunft, Widerspruch, Datenübertragung
- Konzept für Minimalisierung und Terminierung
- Kommunikationskonzept
- Meldekonzept

ISO 27001/2 als Hilfestellung

- Wenn Sie in Ihrem Unternehmen geeignete technische und organisatorische Maßnahmen entwickeln und implementieren oder diese bei einem Auftragsverarbeiter überprüfen wollen, empfiehlt es sich deshalb, auf einen anderen Standard zurückzugreifen: Eine gute Hilfestellung bietet die ISO 27001/2, ein international anerkannter Leitfaden für Informationssicherheits-Maßnahmen.
- Die Norm beschreibt detailliert und ganz konkret „gemeinhin akzeptierte Maßnahmen für die Informationssicherheit“. Ein ISO 27001/2-orientiertes Vorgehen stellt sicher, keine wesentlichen Bereiche zu übersehen und vermeidet Überschneidungen.
- Alternativen sind andere ISMS, wie BSI Grundschutz, ISIS12 oder VdS3473

Meldepflicht bei Datenpannen

Die DS-GVO regelt in den Artikeln 33 und 34 den Umgang bei Datenpannen. Dabei sieht die DS-GVO eine abgestufte Meldepflicht vor:

1. Immer Meldung an die Aufsichtsbehörde, es sei denn, dass die Datenpanne „voraussichtlich nicht zu einem Risiko“ für den Betroffenen führt.
   Meldung sofort, innerhalb 72 Stunden. Unzureichende oder keine/verspätete Meldung wird mit Geldbuße geahndet.
2. Eine Benachrichtigung der betroffenen Person muss dagegen nur dann erfolgen, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht.
3. Keine Meldung, wenn geeignete techn. und organisatorische Maßnahmen vorhanden sind, die den Unbefugten Zugang auf die personenbezogenen Daten praktisch nicht ermöglichen (Verschlüsselung).
   Ebenso kann auf eine Benachrichtigung des Betroffenen verzichtet werden, wenn wirksame Maßnahmen zur Schadensbegrenzung ergriffen wurden und diese das hohe Risiko, das zum Zeitpunkt der Datenpanne bestand, eliminiert haben.

Wie dieses Szenario in der Praxis ablaufen kann, muss insbesondere von Seiten der Aufsichtsbehörden noch geklärt werden. Auf alle Fälle gilt: Immer dokumentieren, immer gut begründen

BayLDA Information

Datenschutzbeauftragter

Grundlagen: Art. 37 DSGVO sowie §38 BDSG 2018

Wann muss ein Datenschutzbeauftragter bestellt werden

Nach DSGVO Art. 37 immer bei einem öffentlichen Verarbeiter.

Nicht-öffentliche Stellen haben nach §38 BDSG 2018 einen Datenschutzbeauftragten zu bestellen, wenn sie …

- in der Regel 20 (früher 10) oder mehr Personen ständig mit der Verarbeitung personenbezogener Daten hauptamtlich beschäftigen,
- Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der DSGVO unterliegen oder
- personenbezogene Daten geschäftsmäßig zum Zweck der (auch anonymen) Übermittlung verarbeiten oder
- bei Kerntätigkeit in der Verarbeitung von Daten besonderer Kategorien DSGVO, Art. 9 und 10

Daneben sollte überlegt werden, ob nicht freiwillig ein DSB bestellt wird, dies ist im Gesetz so vorgesehen, hilft der Kontrolle und reduziert Risiken

Stellung des DSB

- Der Datenschutzbeauftragter ist unmittelbar unterhalb der Geschäftsführung einzuordnen und er ist in seiner Tätigkeit weisungsfrei (Art. 38 Abs.3 DSGVO)
- Zwingend sind dem Datenschutzbeauftragten alle von ihm benötigten Mittel zur Verfügung zu stellen (Art. 38 Abs.2 DSGVO)
- Der Datenschutzbeauftragte kann sowohl externer Dienstleister als auch Mitarbeiter des Unternehmens selber sein wobei auch eine konzernweite Tätigkeit möglich ist (Art. 37 Abs.2,6 DSGVO)
- Bei Bestellung eines betrieblichen Angehörigen sind die Regelungen zum Kündigungsschutz zu beachten.

Aufgaben DSB

Aufgaben ergeben sich im Kern aus den Art. 38, 39 DSGVO ergeben:

- Er ist zentraler Ansprechpartner
  - für die Aufsichtsbehörden und hat die Pflicht mit diesen zusammen zu arbeiten (Art. 39 Abs.1 DSGVO)
  - des Unternehmens gegenüber allen Betroffenen => zwingend Kontaktdaten des Datenschutzbeauftragte nach außen hin bekannt geben, nicht erst auf Anfrage! (Art. 38 Abs.4 DSGVO i.V.m. Art.13 Abs.1 DSGVO)
- Er muss bei allen Maßnahmen eine „Angemessenheitsprüfung“ vornehmen, somit also betriebliche und datenschutzrechtliche Interessen in originärer Abwägung vornehmen (Art. 39 Abs.2 DSGVO)
- Realisieren von Schulungen der Mitarbeiter und die Sensibilisierung hinsichtlich des Datenschutzes erwirken (Art. 39 Abs.2 DSGVO)

Aufsichtsbehörde – Aufgaben (Art. 57, DSGVO)

- Die Anwendung der DSGVO überwachen und durchsetzen
- Die Öffentlichkeit über mögliche Risiken der personenbezogenen Daten aufklären
- Die Regierung über datenschutzrelevante Aspekte beraten
- Verantwortliche und Verarbeiter auf deren Pflichten sensibilisieren
- Mit Beschwerden von Betroffenen und anderen Personen befassen
- Mit anderen Aufsichtsbehörden zusammenarbeiten und ihnen Amtshilfe leisten
- Die Ausarbeitung von Verhaltensregeln fördern (s. Kapitel 7)
- Zertifizierungsstellen benennen und mit den entsprechenden Befugnissen ausstatten
- Jede sonstige Aufgabe im Rahmen personenbezogener Daten
- 1x/Jahr einen Tätigkeitsbericht an das nationale Parlament übermitteln

Bayerisches Landesamt für Datenschutz-aufsicht

Ansbach
24 Mitarbeiter

Präsident

Thomas Kranig

Quelle:
https://www.lda.bayern.de/de/praesident.html

Aufsichtsbehörde – Befugnisse (Art. 58, DSGVO)

- Den Verantwortlichen und ggf. Verarbeiter dazu auffordern sämtliche Informationen bereitzustellen, die für die Prüfung eines Vorgangs erforderlich sind (z.B. Verfahrensverzeichnis und Vereinbarung zwischen Verantwortlichen und Verarbeiter)
- Untersuchungen in Form von Datenschutz-Überprüfungen durchzuführen
- eine Zertifizierungsstelle auf die Einhaltung der Gesetze zu überprüfen
- Sie kann den Verantwortlichen oder den Verarbeiter auf den vermeintlichen Verstoß hinweisen und ihn davor waren, dass das Vorgehen einen Verstoß darstellt und ihn ggf. verwarnen
- Darüber hinaus kann er Verantwortliche und Verarbeiter eine Frist setzen um die Art der Datenverarbeitung in “Einklang mit” der DSGVO zu bringen
- Er kann Zugang zu allen Geschäftsräumen, einschließlich aller datenverarbeitenden Instrumenten erhalten
- Die Anordnung personenbezogene Daten zu löschen oder zu berichtigen
- Eine Zertifizierung zu widerrufen oder eine Zertifizierungsstelle anzuweisen keine Zertifizierungen zu erteilen, wenn die Zertifizierung widerrufen wurde
- Das Verhängen von Geldbußen
- Das Aussetzen einer Übermittlung von Daten an ein Drittland bzw. internationale Organisation
- Jede Aufsichtsbehörde ist schließlich auch dazu berechtigt, Verfehlungen direkt an die zuständigen Justizbehörden weiterzuleiten damit ggf. Verfahren eingeleitet werden können.

Beschwerdeweg

- Beschwerde bzw. Klage einzureichen wurde deutlich vereinfacht
- für alle Mitgliedsstaaten möglichst einheitlich
- Betroffene können sowohl an Ihrem Wohnsitz, als auch an Ihrem Arbeitsplatz (sofern der Arbeitgeber der Verantwortliche ist) Beschwerde einreichen.
- Die Behörden haben den Beschwerdeführer über den Stand dieser Beschwerde zu unterrichten und ihn auf die Möglichkeit eines Rechtsweg vor Gericht hinzuweisen. Ein Rechtsbehelf in Form eines Einspruchs gegen eine Entscheidung steht jedem Bürger zu (Artikel 78 DSGVO).
- Zusätzlich besteht die Möglichkeit sich gemäß Artikel 80 der DSGVO an Organisationen oder Vereine zu wenden, die Datenschutz als Zweck haben.

Bußgelder – Bewertungspunkte (Art. 83, DSGVO)

- Die Art, Schwere und Dauer des Verstoßes im Verhältnis zum Zweck sowie der Art und dem Umfang der Verarbeitung betroffener Daten
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
- Getroffene Maßnahmen des Verantwortlichen oder Verarbeiters um den Schaden zu mindern
- Verantwortung des Betroffenen oder Verantwortlichen unter Berücksichtigung der getroffenen technischen und organisatorischen Maßnahmen
- Frühere Verstöße des Verantwortlichen oder Verarbeiters
- Umfang der Bereitschaft mit den Behörden zur Minderung des Schadens zusammenzuarbeiten
- Einhaltung genehmigter Verhaltensregeln oder Zertifizierungsverfahren
- alle übrigen Umstände die mildernd oder erschwerend hinzukommen könnten bzw. finanzielle Vorteile oder Verluste bedeuten.

Bußgelder - Beträge sollen abschrecken

- Bei Verstößen kann eine Geldbuße von bis zu 10.000.000,00 EUR oder alternativ 2% des weltweit erzielten Jahresumsatzes verhängt werden, je nachdem welcher Betrag höher ausfällt.
- Bei besonders schwerwiegenden Verstößen, wie beispielsweise eine massenhafte und gesetzeswidrige Übermittlung personenbezogener Daten an ein Drittland, können Geldbußen bis zu 20.000.000,00 EUR nach sich ziehen.
- Bei Nichtbefolgung einer Anweisung seitens einer Aufsichtsbehörde können 20.000.000,00 EUR bzw. 4% des weltweit erzielten Jahresumsatz als Strafe festgelegt werden.
- Ordnungswidrigkeiten bei Verstoß gegen Auskunftspflicht in Deutschland: können mit bis zu 50.000 EUR geahndet werden.

Datenschutzerklärung

- Über zwei Drittel aller Datenschutzerklärungen sind laut Aussagen namhafter Juristen mangelhaft → das wird noch mehr werden
- Was ist zu beachten?
  - 1 Klick-Technik (Mit einem Klick an die DSE)
  - Allgemeines, Ansprechpartner, DSB
  - Cookies, Analysetools, Plug-Ins (WP-Plug-Ins)
  - Internetwerbung, Online-Marketing
  - Soziale Medien, Bezahldienste, weiterer Dienste
  - Rechte
- Online-Generatoren, z.B.
  - https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de/
  - https://www.mein-datenschutzbeauftragter.de/datenschutzerklaerung-konfigurator/

Cookie-Policy

- Rigides Kopplungsverbot bei Cookies durch DSGVO

- Für technisch nicht notwendige Cookies gilt:
  - Bevor ein Cookie auf eine Webseite gesetzt wird muss der Benutzer gefragt werden
  - Auch wenn der Benutzer dies nicht erlaubt muss ihm Zutritt zur Seite gewährt werden
- Eigene Cookie-Policy erstellen, z.B.:
  - Cookie Policy
    Cookies sind kleine Textdateien, die auf dem PC des Internetnutzers abgelegt werden. Zweck ist z. B. die Steuerung der Verbindung während Ihres Besuchs auf Internetseiten. Zurzeit verwenden wir ein Cookie, das XYZ. XYZ ermöglich für den Benutzer eine einfache Navigation und eine höhere Sicherheit gegen Angaffe. Das Cookie speichert temporär die Zugriffe des Benutzers. Die Daten werden nach dem Verlassen der Seite wieder gelöscht.

Videoüberwachung

- Grundsätzlich ist eine Videoüberwachung nur zur Aufgabenerfüllung öffentlicher und nicht-öffentlicher Stellen, zur Wahrnehmung des Hausrechts sowie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke gestattet und auch nur dann, wenn das schutzwürdige Interesse der betroffenen Personen nicht überwiegt. (§ 4, Abs. 1 BDSG-neu)
- Bei öffentlich zugänglichen und großflächigen Anlagen, wie Sport- oder Vergnügungsstätten, Einkaufszentren und Parkplätzen oder Fahrzeugen im Schienen- Schiffs- und Busverkehr überwiegt der Schutz von Leben, Gesundheit und Freiheit. Diese Aspekte gelten als besonders schutzwürdige Interessen. Damit soll z. B. Einkaufszentren Videoüberwachung gestattet sein, um die Sicherheit der sich dort befindlichen Bürger zu gewährleisten. (§ 4, Abs. 1 BDSG-neu)
- Wenn Verarbeiter bzw. Verantwortliche auf Videoüberwachung zurück greifen, ist der Umstand der Beobachtung (z.B. Ort und Anlass) sowie Name und Kontaktdaten des Verantwortlichen zum frühestmöglichen Zeitpunkt erkennbar zu machen. (§ 4 Abs. 2 BDSG-neu)
- Für die Speicherung und Verwendung der Daten gilt dieselbe Regelung: Ort und Anlass sowie Kontaktdaten des Verantwortlichen müssen bekannt gegeben werden, ein schutzwürdiges Interesse der betroffenen Personen darf nicht überwiegen. Abweichend von diesem Anlass dürfen die Daten nur dann verarbeitet werden, wenn Gefahren für öffentliche Sicherheit zu erwarten sind bzw. die Verfolgung auf Grund von begangenen Straftaten notwendig ist. Über die Verarbeitung sind die Betroffenen entsprechend zu informieren. Die Daten müssen gelöscht werden, sobald der Verarbeitungszweck erreicht wurde bzw. schutzwürdige Interessen der Personen aufgetreten sind, die einer weiteren Verarbeitung entgegenstehen. (§ 4 Abs. 3, Abs. 4, Abs. 5 BDSG-neu)

Bilder von Personen

- Stillschweigende Einwilligung liegt vor, wenn eine Veröffentlichung offensichtlich ist, z.B. Firma zum Pressefoto, Geld für Foto, …
- Das Gesetz nennt in § 23 KunstUrhG (siehe Anhang) vier Ausnahmen von der Notwendigkeit einer Einwilligung der abgebildeten Person. In diesen Fällen ist keine Einwilligung nötig, wenn man das Bild einer Person veröffentlicht:
  - Bilder von Personen, die schlichtes Beiwerk einer Landschaft oder sonstigen Örtlichkeit darstellen.
  - Bilder von Personen im Bereich der Kunst.
  - Bilder von Personen der Zeitgeschichte kann man ebenfalls ohne Einwilligung verwenden. Damit sind nicht nur Personen gemeint, die aus „Funk und Fernsehen“ bekannt sind. Auch die Bürgermeisterin, der Vereinsvorsitzende oder jemand, der auf einer Veranstaltung etwas darbietet, sind (soweit sie in dieser Funktion auftreten) Personen der Zeitgeschichte.
  - Die letzte Ausnahme, nach der man für die Veröffentlichung eines Fotos regelmäßig keine Einwilligung benötigt, ist die wichtigste für die Öffentlichkeitsarbeit im Verein. (Sie betrifft „Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben“).

Einwilligung für Fotos

- Schriftliche Einwilligung:

  Wichtig ist, dass der Vertragsinhalt auch **tatsächlich angenommen** wurde => deutlich sichtbar positionieren.

  - Für Vereine: Musterklausel aufnehmen in Anmeldungen

    Als Mitglied des Vereins Als Teilnehmer an der Freizeit/am Seminar Als … erkläre ich hiermit mein Einverständnis zur Erstellung von Bildaufnahmen meiner Person im Rahmen von Veranstaltungen des Vereins sowie zur Verwendung und Veröffentlichung solcher Bildaufnahmen ausschließlich zum Zwecke der öffentlichen nicht-kommerziellen Berichterstattung über das Vereinsleben.

- Mündliche Einwilligung:

  Ist möglich. Die Person, die vor, während oder nachdem sie fotografiert wurde, erklärt hat, mit der Verwendung und Veröffentlichung des Bildes einverstanden zu sein, hat wirksam eingewilligt.

- Konkludent (durch schlüssiges Verhalten):

  Auch ohne sich konkret zu äußern, kann eine Person ihre Einwilligung dadurch "erklären", dass sie sich im Wissen der Erstellung und der späteren Verwendung der Fotografie hierfür **bereitwillig zur Verfügung** stellt (Unbedingt klarstellen, **wofür** das Foto erstellt und **wie** und **wo** es verwendet wird)

Verzeichnis von Verarbeitungstätigkeiten

- Art. 30 DSGVO fordert dies grundsätzlich
  - Theoretische Freistellung für Unternehmen mit weniger als 250 MA, die nur gelegentlich mit personenbezogenen Daten hantieren und auch nicht mit besonderen personenbezogenen wie Religionszugehörigkeit oder Gesundheitsdaten.
  - Besser: einfach machen, das gibt auf alle Fälle einen guten Überblick
- Es gibt nur eines, dieses ist nicht öffentlich, dient der eigenen Qualitätskontrolle und muss der Aufsichtsbehörde auf Verlangen vorgelegt werden.
- Es ist in deutscher Sprache regelmäßig, schriftlich/elektronisch zu führen und aktuell zu halten.
- Der Mindestinhalt ist in Art. 30, DSGVO beschrieben. Ein Muster kann auf unserer Webseite heruntergeladen werden.

Auftragsverarbeiter gut auswählen

Stellen Sie unbedingt sicher, dass ihr Auftrags(daten)verarbeiter

1. auf ihre Weisung handelt,
2. dies nach einem gültigen A(D)V-Vertrag tut,
   Sie entsprechende Kontrollrechte haben und
   denken sie bei der Auftragsvergabe bereits an die Beendigung
3. die vereinbarten TOMs einhält,
4. das Verzeichnis der Verfahrenstätigkeiten lückenlos pflegt,
5. gesetzliche Meldepflichten einhält.

Zusammenfassend

Wo überall verarbeite ich personenbezogene Daten?	Bestandsaufnahme intern Auftragsverarbeiter inkludieren
Verarbeite und nutze ich die Daten gesetzeskonform? Auf welcher Grundlage?	Awarenessgenerierung, Anpassungen von AGB, DSE, … DSB bestellen (ggfs.)
Kann ich auf alle personenbezogenen Daten zugreifen, diese berichtigen, löschen, Auskunft geben?	Verfahrensüberprüfung, Vertragsanpassungen, Verfahrensverzeichnis
Sind ausreichend Maßnahmen zur Daten-Sicherheit getroffen?	Tech. & organische Maßnahmen Review, Kommunikation
Wie stelle ich dauerhaft sicher, dass Vorgaben eingehalten werden und dass ich bei Verletzungen schnell informiere?	Handlungsanweisungen Prozesse definieren, kommunizieren & testen ISMS (27001 o.dgl.)

Vorgehen bei Sicherheitsvorfällen

secobit

- Halte Dich an die vorgegebene Vorgehensweise (calm down!)
- Sichere alle Systeme, arbeite auf Sicherungen, wenn du gerichtsverwertbar bleiben willst
- Überlege ob es wichtiger ist das System gereinigt zu bekommen oder den Angreifer zu greifen
- Unterbreche die Verbindungen und schärfe die Kommunikation (Firewall-Regeln)
- Untersuche die Logs der betroffenen Systeme, versuche den Angriff zu verstehen
- Prüfe, ob es leichter ist ein Backup einzuspielen oder die Systeme zu reiningen
- Analyse den Vorfall und die genauen Auswirkungen
- Denke daran, dass ein sichtbarer Vorfall nur ein Teil des Angriffs sein könnte (Eisberg) und dass der Angreifer sich viel tiefer eingenistet hat.
- Melde den Vorfall ggfs an Meldestellen

Ein Tipp zum Schluss

- ✓ Sichere Passwörter und Geheimhaltung der Passwörter
- ✓ Virenschutz und Personal Firewall
- ✓ E-Mail Sicherheit – Signatur und Verschlüsselung
- ✓ Datenschutz und Verschlüsselung
- ✓ Aufklärung und Üben von Social Engineering
- ✓ Sicherer Umgang mit Mobilgeräten und Datenträgern
- ✓ Akzeptanz hochhalten: Ansprechpartner, wenn was auffällt (nicht abmahnen)
- ✓ Mitarbeiterschulungen und Awareness-Maßnahmen
  - ✓ Teil einer umfassenden Sicherheitskultur sein.
  - ✓ Die Unternehmensleitung lebt Sicherheit vor ("Sicherheit ist Chefsache")
  - ✓ organisatorisch strukturierte Sicherheitsmaßnahmen
  - ✓ Kampagnen erhöhen die Sicherheit

Ihre Mitarbeiter sind der Schlüssel zur Sicherheit

Wo finden Sie weiterführende Infos?

- Gute Informationen finden Sie immer in den Kurzpapieren der DSK (Datenschutzkonferenz) https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/DSGVO_Kurzpapiere.html
- Oder auf der Seite der Landesdatenschutzbeauftragten, wie z.B. https://www.lda.bayern.de/de/veroeffentlichungen.html

Wenn Sie weitere Beratung wünschen …

Wir beraten Sie gerne bei Fragen zum Datenschutz, erarbeiten Vorschläge zur wirksamen Verbesserung der Sicherheit oder unterstützen bei der Einführung eines Informations-Management-Systems wie der ISO27001

- nicht nur während der Planung
- sondern kümmern uns auch um die Realisierung

Starten Sie noch heute und nehmen Sie Kontakt zu uns auf

https://secobit.de

Email: 4you@secobit.de

Tel.: 0821/5675041

Thomas Schkoda & Harry Schäfle

Vielen Dank für Ihre Aufmerksamkeit

Wir freuen uns über eine Kontaktaufnahme
4you@secobit.de