AETeam
Allgemeine EDV-Beratung GmbH

Die Programm-Zuschneider: individuell, schnell, clever

Persönliche Daten rechtssicher schützen

25. Mai 2018

Die EU-DSGVO trifft alle

D.O.T Software
Data Oriented Testing

cobra® CRM
schneller erfolgreich

Im Mai 2018 tritt die neue EU-Datenschutzgrundverordnung in Kraft.

Ihr Ziel ist, jedem einzelnen Bürger der EU wieder mehr Kontrolle darüber zu geben, wer wozu und wie persönliche Daten verwendet.

Unternehmen und Organisationen jeder Grösse müssen die Regeln der EU-DSGVO einhalten, anderenfalls drohen "abschreckende" Strafen.

Es bleiben weniger als 200 Tage, diese Regeln kennenzulernen und umzusetzen!

Der Countdown läuft.

Vorwort

Gute Waren und Dienstleistungen anzubieten ist heute nicht mehr genug. Das Angebot des Wettbewerbs ist nur einen Mausklick entfernt. Das macht es wichtiger als je zuvor, ***stabile und tragfähige Kundenbeziehungen*** aufzubauen. Dafür benötigt man präzise Informationen über seine Kundschaft und Interessenten. Nur so kann man sie gezielt ansprechen, ihre Bedarfe frühzeitig erkennen und seine Strategie sauber planen. Ein Newsletter mit aktuellen branchenspezifischen Informationen gehört heutzutage fast schon zum "Guten Ton".

Gute und verlässliche Daten sind damit zu einem der wichtigsten Güter in der Wirtschaft des 21. Jahrhunderts geworden. Diese neue Situation wurde auch in der Politik erkannt und damit ist der Umgang mit Daten - insbesondere personenbezogenen Daten - in den Fokus der Gesetzgeber gerückt.

Im Ergebnis tritt am ***25. Mai 2018*** die EU-Datenschutzgrundverordnung (EU-DSGVO) in Kraft. Dieses Regelwerk regelt den Umgang mit personenbezogenen Daten ***deutlich strenger***, als seine Vorgänger. Es verlangt von uns Unternehmern ***Vorsorge, Umsicht und Rechenschaft*** über die Speicherung und Verwendung von personenenbezogenen Daten. Und es droht bei Nichtbeachtung mit ***"abschreckenden" Strafen***.

Dieses Whitepaper gibt eine ***Übersicht*** über die wichtigsten Aspekte der EU-DSGVO, die Sie als Unternehmer beachten müssen. Es wurde von den Autoren nach bestem Wissen erstellt und führt in die Materie ein. Es ersetzt keinesfalls die fachliche Beratung durch einen ***kompeteten und zertifizierten Datenschutzfachmann***. Vielmehr soll es Ihnen helfen, schnell eine gute Kommunikation mit Ihrem Datenschutzbeauftragten aufzubauen, weil Sie die Grundbegriffe schon kennen.

Der vollständige Text der Verordnung steht im Internet zur Verfügung. Zum Beispiel auf der Website des Landesdatenschutzamtes Bayern:
https://www.lda.bayern.de/de/datenschutz_eu.html.

Für die bessere Lesbarkeit werden meist nur die männliche oder die weibliche Form für Personen verwendet. Es sind aber in allen Fällen beide Geschlechter gemeint.

Zusammenfassung

Die EU-DSGVO sieht vor:

- Stärkung der Kontrolle der EU-Bürger über die ***Verbreitung ihrer personenbezogenen Daten*** und engere Grenzen für deren Verwendung hinsichtlich der Privatsphäre, des Profiling, der Aufbewahrung, der Verarbeitung und Verbreitung dieser Daten.
- Klar definierte Rechte für die Portabilität der Daten mit dem expliziten Recht von Personen, ihre ***persönlichen Daten zu entziehen***.
- ***Verantwortlichkeit*** der Datenverarbeiter, unabhängig davon, ob sie selbst die Daten sammeln und speichern oder dafür lediglich beauftragt sind.
- Sie sind in allen Fällen verpflichtet, ***präventive Massnahmen*** gegen Datenverlust oder -missbrauch zu ergreifen.
- Besseres Verständnis für die Regelungen: ***klare, leicht verständliche Sprache***, um sie für ein breites Publikum verständlich zu machen.
- ***Harmonisierung*** der verschiedenen Datenschutz-Direktiven, um die Aufgaben bei der Compliance zu vereinfachen und letztendlich Kosten zu sparen.
- ***Bessere Zusammenarbeit*** zwischen den Datenschutz-Behörden und den Datenschutzbeauftragten in den Organisiation.

Hintergrund

Die digitale Wirtschaft und unsere permanente Netzwerkanbindung hat den globalen Fluss von Daten dramatisch verändert. Deshalb wird der ***Schutz von persönlichen Daten*** sowohl im nationalen, wie auch im internationalen Bereich ***immer wichtiger***.

Nach mehreren Jahren der Vorbereitung wurde im April 2016 die neue General Data Protection Regulation (GDPR - in Deutschland: ***EU-DSGVO***) beschlossen. Ihr Ziel ist es, die zahlreichen verschiedenen Regelungen der einzelnen EU-Mitgliedsstaaten zu harmonisieren und damit die Rechte der Bürger in der digitalen Wirtschaft zu stärken. Diese Regelung tritt im Mai 2018 ***in der gesamten EU in Kraft***. Sie braucht nicht weiter in den Ländern beschlossen zu werden.

Die GDPR wirkt auch „extraterritorial“: sie hat ***international Gültigkeit*** für alle Organisationen, die Daten von EU Bürgern verarbeiten, verwenden oder speichern. Die GDPR hat nicht nur sehr strenge Regeln, auch in der Höhe der Strafen, die bei Zuwiderhandlungen verhängt werden können, ist sie mit maximal 20 Millionen € oder 4 % des weltweiten Umsatzes (jeweils der höhere Wert zählt) ein echter Meilenstein.

Die Direktive verlangte von jedem EU Mitgliedstaat, eine ***nationale Organisation*** zu gründen, mit der Aufgabe, alle Aktivitäten im Zusammenhang mit der Verarbeitung persönlicher Daten zu überwachen. In Großbritannien ist dies z.B. das *Information Comissioner's Office* (ICO) während in Irland das *Office of the Data Protection Commissioner* diese Aufgaben wahrnimmt. In Frankreich wiederum ist es die *CNIL* und in Holland die *Dutch Data Protection Authority*. Eine vollständige Übersicht über die verschiedenen nationalen Organisationen ist hier verfügbar: https://www.cnil.fr/en/data-protection-around-the-world.

Die neue EU-DSGVO verstärkt die Direktive noch einmal. Sie verlangt, dass Firmen ***mindestens einen Datenschutzverantwortlichen*** benennen, der die Verantwortung dafür trägt, dass dem Datenschutz Rechnung getragen wird. Diese Person dient als Verbindung zu den nationalen Aufsichtsbehörden.

Die EU-DSGVO enthält auch Regelungen für eine ***intensivere Zusammenarbeit*** zwischen den nationalen Datenschutzbehörden. Europäische Behörden können jetzt gemeinsam darüber entscheiden, ob eine Organisation die Regeln einhält oder nicht. Sie können auch Strafen bei Nichteinhaltung verhängen. Art. 68 des Regelwerks sieht die Gründung eines *European Data Protection Board* (EDPD) vor. Dieses soll die derzeit noch existierenden Arbeitsgruppen (Art. 29 oder WP 29) ersetzen. Es setzt sich aus Delegierten von 28 Überwachungsbehörden zusammen.

Strafen

Ein wichtiger Unterschied zur alten Direktive ist die ***Höhe der Strafen***, die gegen Organisationen verhängt werden können, die keine hinreichenden Mechanismen zum Schutz der persönlichen Daten von EU Bürgern unterhalten. Diese können bis zu 20 Millionen Euro oder 4 % des weltweiten Umsatzes der Organisation erreichen. Die Gerichte sind zwar frei in ihrer Entscheidung über die Höhe der Strafe, aber die Verordnung verlangt ausdrücklich, dass die Strafen "***abschreckend***" sein sollen.

Gültigkeitsbereich

Die EU-DSGVO erweitert den Gültigkeitsbereich des EU Datenschutzrechtes in zwei wichtigen Bereichen:

1. Auftragdatenverarbeiter

Zusätzlich zu den schon bisher gültigen Regeln für „Verantwortliche“ (Auftraggeber, der bestimmt, welche Daten wie zu verarbeiten sind) gibt die EU-DSGVO erstmalig Regeln für die „Auftragsdatenverarbeiter“ (Personen oder Organisationen, die persönliche Daten für andere verarbeiten) vor. (Der Begriff wird auch gelegentlich mit "Auftragsverarbeiter" abgekürzt.)

2. Internationale Ausrichtung

Die EU-DSGVO gilt für jede Verarbeitung von persönlichen Daten von Personen, deren ***Wohnsitz in der EU liegt***, wenn sie in Bezug zu einem Waren- oder Dienstleistungsverkehr stehen oder ihr Verhalten nach verfolgen sollen ("Profiling"). Dabei ist es unerheblich, ob die Waren oder Dienstleistungen kostenpflichtig sind oder nicht.

In der Praxis heißt das, dass viele Organisationen, sowohl innerhalb, als auch außerhalb der EU, ***jetzt direkt von den Regelungen betroffen sind***, was vorher oft nicht der Fall war. Das gilt zum Beispiel für Auftragsverarbeiter innerhalb der EU oder auch Verantwortliche außerhalb der EU, die entweder ***EU-Bürgern etwas verkaufen oder ihr Nutzerverhalten verfolgen*** wollen. In diesen Fällen ist die EU-DSGVO eine große Umstellung und ihre Umsetzung wird ein ziemlicher Kraftakt.

In den USA gibt es das *EU-U.S. Privacy Shield Framework*. Dieses hilft Firmen, bei der Übertragung von persönlichen Daten von der EU in die USA die EU-Datenschutzbestimmungen einzuhalten. Privacy Shield ersetzt das frühere Safe Harbor-Abkommen[1], das von europäischen Gerichten aufgehoben wurde. Es ist ein freiwilliges Programm und wird von der Federal Trade Commission (FTC) in Washington, DC unterstützt.

[1] *"Safe Harbor": Vereinbarung über die Speicherung und Verarbeitung von persönlichen Daten von EU-Bürgern durch US-Firmen ausserhalb der EU. Wurde im Jahr 2015 von Europäischen Gerichtshof aufgehoben.*

Die europäische Datenschutz-Timeline

1995	EU-Datenschutz-Direktive (95/46/CE)
2000	"Safe Harbor" Vereinbarung zwischen dem US-Wirtschaftsministerium und der Europäischen Union
2012	EU-Kommission schlägt eine Reform des Datenschutes vor
2014	Der Europäische Gerichtshof bestätigt das "Recht auf Vergessen"
Oktober 2015	Der Europäische Gerichtshof hebt Safe Harbor auf
Dezember 2015	Europaparlament, Rat und Kommisision einigen sich auf eine neue Vereinbarung zu den Datenschutz-Regeln
April 2016	Das Europaparlament verabschiedet die neuen GDPR
Juli 2016	"Privacy Shield" wird von der Europäischen Kommission als Ersatz für Safe Harbor angenommen
25. Mai 2018	Die neuen, strengen Regeln der DSGVO treten in Kraft!

Worum geht es bei der Neuregelung?

Die EU-DSGVO handelt vom Schutz der fundamentalen Rechten von Personen über ihre persönlichen Daten.

Sie enthält Bestimmungen über

- die Zustimmung zur Speicherung von
- die Information über die
- den Zugang zu den
- die Korrektur von

personenbezogenen Daten, die von Organisationen über sie gespeichert und verarbeitet werden.

Was sind die wichtigsten Eckpunkte?

Verankerung des Datenschutzbeauftragten

Organisationen, die personenbezogene Daten speichern oder verarbeiten, müssen einen ***Datenschutzbeauftragten*** benennen, der beruflich qualifiziert ist und Fachwissen auf dem Gebiet des Datenschutzrechts unter Datenschutzpraxis besitzt.

Rechenschafts-[2] und Vorsorgepflicht für Organisationen

Sie verpflichtet die Auftraggeber dazu, ***ihre Compliance nachzuweisen***. Eines der neuen Prinzipien der EU-DSGVO ist die Forderung, den Schutz der Privatsphäre als Standard ***im Design*** zu verankern ("privacy by design and privacy by default"): die Auftraggeber müssen sicherstellen, dass

- der Schutz der Privatsphäre Bestandteil des grundlegenden Designs von Geschäftsprozessen und Anwendungen ist (**privacy by design[3]**)
- personenbezogene Daten nur in dem für den jeweiligen Geschäftsvorfall mindestens erforderlichem Umfang erfasst und verarbeitet werden (**privacy by default[4]**).

Das Recht auf Information und Datenübertragbarkeit (Artikel 20)

Jede Person hat das Recht, die über ihn oder sie ***gespeicherten personenbezogenen Daten übergeben zu bekommen*** und sie einem anderen Auftraggeber zu übergeben.

Das Recht auf Löschung („Vergessenwerden") (Artikel 17)

Natürliche Personen haben das Recht, jederzeit das ***Löschen*** ihrer persönlichen Daten zu verlangen. In diesem Fall sind alle von dieser Forderung betroffenen Auftraggeber verpflichtet, die für sie tätigen Auftragsdatenverarbeiter darüber zu informieren.

Organisationen, die mit personenbezogenen Daten arbeiten werden intensiver kontrolliert (Artikel 7)

Der Auftraggeber ist verpflichtet, die Zustimmung der Person zur Speicherung und Verwendung ihrer Daten zu dokumentieren und nachzuweisen.

---

[2] *Rechenschaftspflicht: Pflicht der Organisationen, Mechanismen und interne Prozeduren einzuführen, mit denen der Nachweis geführt werden kann, dass die Organisation die Datenschutzbestimmungen einhält, die die Rückverfolgbarkeit der Datenverarbeitungsprozesse garantieren und die die Transparenz für die aufsichtsführenden Behörden sicher stellen.*

[3] *Privacy by design: der Schutz personenbezogener Daten ist bereits Bestandteil des Designs von Geschäftsprozessen, Technologien, täglicher Verwaltungsabläufe und der Architektur des Informationssystems. Ziel ist es, den Schutz der Privatsphäre präventiv und proaktiv vorzusehen und nicht erst auf Datenpannen reagieren zu müssen.*

[4] *Privacy by default: das Sammeln von personenbezogenen Daten darf nur auf Grundlage der gesetzlichen Regelung erfolgen und muss begrenzt sein auf die Daten, die unbedingt für den einzelnen Vorgang erforderlich sind. Informations– und Kommunikationstechnologien sollen grundsätzlich mit nicht-identifizierbaren Interaktionen und Transaktionen beginnen. Wo immer möglich sollen die Identifizierbarkeit und die Beobachtbarkeit von personenbezogenen Daten weitestgehend minimiert werden.*

Das Recht, in einer leicht zugänglichen, klaren und einfachen Sprache informiert zu werden (Artikel 12, 13 and 14)

Die Informationen, die von einem Auftraggeber an eine Person übergeben werden, müssen ***zutreffend, transparent und verständlich*** sein. Dafür muss der Auftraggeber eine klare und einfache Sprache verwenden.

Das Recht über eine Datenpanne informiert zu werden (Artikel 33 and 34)

Im Fall eines Datenverlustes oder wenn der Schutz personenbezogener Daten verletzt wurde muss der Auftraggeber die Aufsichtsbehörde unverzüglich – nach Möglichkeit ***innerhalb von 72 Stunden*** – detailliert darüber informieren, so dass angemessene Massnahmen eingeleitet werden können.

Die von der Datenpanne ***betroffenen Personen müssen auch informiert*** werden (Artikel 34): "Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person". Wenn der Auftraggeber in Hinblick auf die Rechte und die Freiheit der Betroffenen die Datenpanne für gefährlich einschätzt, dann ist er verpflichtet, sie umgehend darüber zu informieren.

Die ***Auswirkungen einer Datenpanne*** auf die Privatsphäre der Betroffenen müssen geprüft werden, um ihnen im Hinblick auf den angerichteten Schaden ***angemessene Lösungen anzubieten.***

Grenzen der Profilierung (Artikel 21)

Jede Person hat jederzeit das Recht, auf Grund ihrer besonderen persönlichen Situation der Verarbeitung ihrer personenbezogenen Daten, inklusive der Profilierung, zu ***widersprechen***.

Damit wird die Praxis eingeschränkt, die Leistung einer Person bei der Arbeit zu analysieren oder vorherzusagen. Auch die Analyse des Kaufverhaltens, der wirtschaftlichen Situation, der Gesundheit oder biometrischer Daten wird hier eingeschränkt sowie die automatische Verarbeitung der persönlichen Daten.

Im Allgemeinen darf ***Profilierung nur mit aktiver Zustimmung*** einer Person durchgeführt werden.

Besonderer Schutz für Kinder (Artikel 8)

Für das Speichern und Verarbeiten von Daten von Personen unter 16 Jahren ist in jedem Fall das ausdrückliche ***Einverständnis der oder des Erziehungsberchtigten*** einzuholen.

Der Schutz der Privatsphäre ist die Norm

Alle Organisationen sind verpflichtet, Vorkehrungen zu treffen, die dafür sorgen, dass die Speicherung und Verarbeitung von personenbezogenen Daten auf das ***erforderliche Minimum reduziert*** bleibt. Dieser Schutz der Privatsphäre ist bereits beim Design von Produkten und Dienstleistungen grundsätzlich vorzusehen.

Was ist zu tun?

Der erste Schritt zur Compliance mit der EU-DSGVO ist selbstverständlich die Benennung eines ***Datenschutzbeauftragten***.

Dies kann eine Person im Unternehmen sein, die entsprechend ausgebildet wird. Für mittlere und kleine Unternehmen kann es aber sinnvoller sein, einen externen Datenschutzbeauftraten zu bestellen.

Unter anderen hält der Bundesverband der Datenschutzbeauftragten (BvD – www.bvdnet.de) eine Liste von kompetenten Personen dafür vor. Der Datenschutzbeauftragte wird Ihr Unternehmen dabei unterstützen, die Regelungen der EU-DSGVO für Ihr Unternehmen angemessen umzusetzen.

Gemeinsam mit dem Datenschutzbeauftragten müssen Sie den Umgang mit personenbezogenen Daten im Hause analysieren und dokumentieren. Unter anderem ist zu klären und zu beschreiben:

- Welche personenbezogenen Daten werden bei Ihnen gesammelt, verarbeitet, weitergegeben? Warum?
- Wie gehen Sie mit Anfragen zu personenbezogenen Daten um: welche werden bei Ihnen gespeichert? Wer hat Zugriff auf sie? Warum? An wen wurden sie weitergegeben? Was passiert, wenn eine Person Sie auffordert, ihre Daten zu löschen?
- Wie werden die Mitarbeiter in Ihrem Hause im Umgang mit personenbezogenen Daten geschult?

Diese (und noch viele weitere Fragen) müssen dokumentiert sein. Wenn das Amt für Datenschutz Sie fragt, dann müssen Sie diese Definitionen und Verfahrensanweisungen zeigen können.

Software, die hilft

Die Anforderungen der EU-DSGVO können nicht umgangen werden. Ab dem 25.05.2018 müssen sie eingehalten werden und es gibt keine Übergangsfrist.

Deshalb haben wir bei AETeam uns nach Software umgesehen, die kurzfristig einsetzbar ist und bei der Erfüllung der Anforderungen hilft.

Das sind zwei Produkte:

cobra CRM
schneller erfolgreich

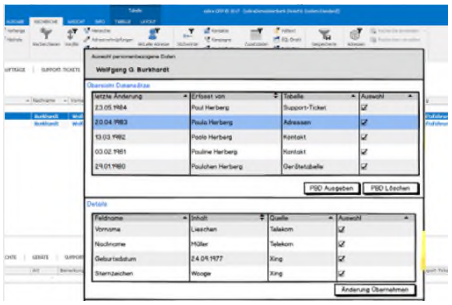
Kunden-Beziehungs-Pflege
auf höchstem Niveau

D.O.T Software
Data Oriented Testing

Anonymisierung für Software-
Tests und Big Data

Cobra CRM – Kundenbeziehungspflege "Datenschutz ready"

Wenn Sie heute Ihre Kundenbeziehungen noch mit einem E-Mail-, einem Textprogramm und einer Tabellenverarbeitung pflegen, dann wird die Umsetzung der EU-DSGVO für Sie sehr mühsam und zeitaufwändig.



Cobra CRM ist ein umfangreiches state-of-the-art Programm zur Pflege von Kundenbeziehungen und Bestandteil des AETeam-Portfolios. In der neuesten Version werden Felder, die personenbezogene Daten enthalten DSGVO-konform überwacht. Sie können auf Knopfdruck Berichte zu den gespeicherten Daten erstellen und auch das Löschen solcher Daten nach den Kriterien der EU-DSGVO geht auf Knopfdruck. Die Vorgaben der Verordnung sind damit komfortabel gelöst.

Weitere Informationen finden Sie unter:

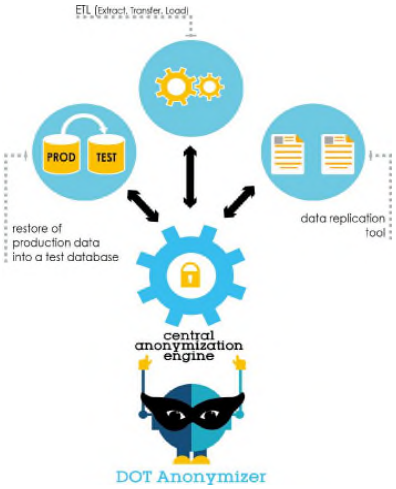
https://www.cobra.de/datenschutz-2018/uebersicht-datenschutz-2018/

Für Entwickler: Anonymisierung von Testdaten

Wenn Sie selbst für Ihr Unternehmen Software entwickeln oder Software entwickeln und vertreiben, dann gehört das Testen Ihrer Programme einfach dazu.

Die bislang gepflegte Tradition, "einfach" einen Teil der Produktionsdaten in das Testsystem zu kopieren steht aber im Konflikt mit den EU-DSGVO – Vorgaben. Diese verlangen, dass Programmierer oder Personen, die mit dem Test oder der Qualitätssicherung von Programmen beschäftigt sind, keinen Zugriff auf Produktionsdaten haben. Kurz gesagt: es geht den Entwickler nichts an, wie hoch der Dispo seines Nachbarn ist.

Das Produkt DOT-Anonymizer der französischen ARCAD Software Group hilft hier weiter. Es gibt Organisationen die Möglichkeit, individuell auf sie zugeschnittene Pseudonymisierungs- und Anonymisierungstechniken unternehmensweit einzusetzen und in den Datenfluss zu integrieren. Damit können Unternehmen problemlos auch die strengen Vorgaben der EU-DSGVO einhalten.



DOT-Anonymizer schützt die Vertraulichkeit der Daten, indem die persönlichen Elemente anonymisiert werden. Trotzdem bleiben die Daten weiterhin verwendbar, denn ihr Format und Typ bleiben erhalten.

Die zentrale Anonymisierung – Engine von **DOT-Anonymizer** erlaubt es, die Daten **über alle Datenbanken** einer Organisation hinweg zu schützen.

Weitere Informationen finden Sie unter:

https://arcadsoftware.com/solutions/data-masking/

Das Unternehmen AETeam GmbH

Seit 1995 betreuen wir ein ***sorgfältig ausgewähltes Portfolio*** von Cross-Industry Produkten, wie z.B. die hier vorgestellten Produkte *cobra CRM* und *DOT Anonymizer*.

Wir unterstützen unsere Kunden bei der Implementierung, Anpassung und Pflege dieser Produkte. Dabei legen wir Wert darauf, dass die von uns vertretenen Produkte in ihrem Bereich ***"best of breed"*** sind.

Als ***offizielle Business Partner*** pflegen wir intensive Beziehungen zu den jeweiligen Softwarelieferanten zum Nutzen unserer Kunden.

So erreichen Sie uns:

Telefonisch: +49 40 357 09 100
Per E-Mail: vertrieb@aeteam.de
Per Fax: +49 40 357 09 106
Im Web: www.aeteam.de

AETeam – Allgemeine EDV-Beratung GmbH
Richardstrasse 84
22089 Hamburg