techbold

EU-DATENSCHUTZ-GRUNDVERORDNUNG LEITFADEN

INHALT

01. EINLEITUNG 3
Harmonisierter Datenschutz 3

02. WEN BETRIFFT DIE DSGVO? 4
Sachlicher & räumlicher Anwendungsbereich 4
Personenbezogene Daten 4

03. NEUE PFLICHTEN FÜR UNTERNEHMEN 5
Datenschutz-Folgeabschätzung 5
Verzeichnis von Verarbeitungstätigkeiten 6
Datenschutzbeauftragter 6
Meldepflicht bei Datenschutzverletzungen 6

04. INFORMATIONSPFLICHTEN & DIE RECHTE BETROFFENER 7
Leichtere Ausübung der Rechte 7

05. WICHTIGE BEGRIFFE 9

06. SCHLAGWÖRTER / INDEX 12

01. EINLEITUNG

Jetzt wird's aber wirklich ernst. Nachdem die DSGVO 2016 in Kraft getreten ist, wird die EU-Datenschutzgrundverordnung (DSGVO) ab 25. Mai 2018 auch endgültig angewandt.

Schikane, Schreckgespenst oder gar ein Segen für alle EU-Bürger? Wie so oft im Leben lässt sich diese Frage auch in Sachen DSGVO nicht wirklich eindeutig beantworten – im Grunde ist's ja auch von allem ein bisschen. Abgesehen davon, dass eine solche Diskussion ohnehin müßig ist: Die Verordnung ist in Kraft, jetzt gilt es das Beste daraus zu machen. Eines ist jedenfalls sicher, wirklich neu erfunden wird der Datenschutz auch mit der DSGVO[1] nicht. Zahlreiche Prinzipien, die im Österreichischen Datenschutzgesetz (DSG 2000)[2] schon bisher zu finden waren, bleiben uns zukünftig auch in der DSGVO erhalten. Wie etwa der „Erlaubnisvorbehalt", wonach man die Erlaubnis einer Person benötigt, um seine Daten entsprechend verarbeiten zu dürfen. Oder das Prinzip der „Zweckbindung", welches besagt, dass man die Daten nur zu jenem Zweck verarbeiten darf, für den sie eigentlich erhoben wurden.

Freilich gesellen sich mit der DSGVO auch viele neue Rechte und Pflichten hinzu. Vor allem die Informationspflichten (Recht auf Datenauskunft) und die Betroffenenrechte (Recht auf „Vergessen") erfahren in der DSGVO eine deutliche Erweiterung beziehungsweise sind überhaupt neu. Ebenso wie die Maßnahmen, die im Falle eines Datenverlusts oder Datenmissbrauchs zu erfolgen haben. Über dem ganzen Datenschutz-Konstrukt schwebt zudem das Damoklesschwert drakonischer Strafen: Bis zu maximal vier Prozent des (globalen) Jahresumsatzes bzw. 20 Mio. Euro (je nachdem, welcher Betrag höher ist) kann die Missachtung der DSGVO ein Unternehmen im schlimmsten Fall der Fälle kosten. Angesichts der Tatsache, dass Verstöße gegen das Datenschutzgesetz bislang nur mit einem sprichwörtlichen Klaps auf die Finger bestraft wurden, hinterlassen diese Zahlen schon einen gehörigen Eindruck – selbst bei größeren Unternehmen.

HARMONISIERTER DATENSCHUTZ

Auch wenn viele Unternehmen, vor allem ob des technischen Aufwands und der dafür nötigen Investitionen, derzeit nicht sonderlich gut auf die DSGVO zu sprechen sind, die Verordnung nur zu verteufeln wäre ungerecht. Immerhin bedeutet diese doch eine weitgehende Vereinheitlichung des europäischen Datenschutzrechtes. Bislang war der Datenschutz in den nationalen Gesetzgebungen (freilich auf Basis der bereits bestehenden EU-Datenschutzrichtlinie) geregelt, was aber trotzdem oft erhebliche Unterschiede mit sich brachte. Österreichische Unternehmen (etwa Online-Händler), die in mehreren EU-Ländern tätig sind oder waren, können zumeist ein Klagelied hiervon singen.

Im Gegensatz dazu ist die Datenschutz-Grundverordnung in allen Mitgliedsstaaten direkt geltendes Recht und wird demzufolge nur noch geringe Unterschiede aufweisen. Gering deswegen, weil einige Staaten während der jahrelangen Verhandlungen auf so genannte „Öffnungsklauseln" bestanden haben, um den nationalen Gesetzgebern Spielräume zu bieten. Diese betreffen aber kaum den eigentlichen Kern der DSGVO, sondern sind eher punktuelle Konkretisierungen von (Rand-)Bestimmungen bzw. Abläufe und Verfahren – ein nachträgliches Aufweichen oder Verschärfen von DSGVO-Regelungen ist damit allerdings kaum möglich. Übrigens: Hierzulande sind die Ergebnisse dieser „Öffnungsklauseln" in einer Novelle des österreichischen Datenschutzgesetzes 2000, dem so genannten „Datenschutz-Anpassungsgesetz 2018"[3] zu finden. Dieses wird – wenig überraschend – ebenfalls mit 25. Mai 2018 in Kraft treten.

[1] http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016R0679

[2] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001597

[3] https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf

02. WEN BETRIFFT DIE DSGVO?

Um es kurz zu machen: Fast alle Unternehmen. Sobald nämlich personenbezogene Daten natürlicher Personen (etwa Kunden- oder Mitarbeiterdaten) verarbeitet werden, beginnen die Bestimmungen die DSGVO zu greifen. Für Daten von juristische Personen (Firmen usw.) gelten die Regeln übrigens nicht. Klingt jetzt sehr einfach, ist es aber irgendwie doch nicht. Zahlreiche juristische Feinheiten und – vor allem – die recht weit gefassten und teilweise schwer durchschaubaren Begriffsdefinitionen sorgen dafür, dass es bei der Umsetzung der Verordnung garantiert nicht langweilig wird. Aus diesem Grund ist es auch unumgänglich, einen kurzen Blick auf eben jene Begriffe zu werfen.

SACHLICHER & RÄUMLICHER ANWENDUNGSBEREICH

Ausschlaggebend dafür, ob man unter die DSGVO fällt, ist der so genannte **sachliche Anwendungsbereich**[4]. Im feinsten Gesetzes-Deutsch heißt es dazu in Artikel 2 DSGVO:

„Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“

Unternehmen, die noch auf die gute alte handschriftliche Kundenkartei (sprich: „nichtautomatisierte Verarbeitung“) setzen, können jetzt übrigens NICHT aufatmen. Dafür sorgt schon allein die Formulierung „…gespeichert werden sollen“. Demnach reicht bereits die Absicht, personenbezogene Daten irgendwann in ein Dateisystem aufzunehmen, aus, um der DSGVO zu unterliegen. Zur „automatisierten Verarbeitung“ zählen wiederum Computer, Smartphones, Kameras, Webcams, Dashcams, Scanner oder Kopierer. Das heißt auch: Jede Benutzung von Computer, Internet, E-Mail kann also zur Anwendbarkeit der DSGVO führen, sobald personenbezogene Daten betroffen sind.

Mitunter etwas missverständlich kann in diesem Sinne auch der Begriff **Verarbeitung**[5] sein. Dazu zählt laut DSGVO nämlich jeder Vorgang, der in Zusammenhang mit personenbezogenen Daten steht. Also das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen aber auch die Vernichtung von Daten. Im Grunde also alle Tätigkeiten, die man beispielsweise in einer normalen Kundenkartei durchführt.

Schneller und einfacher erklärt ist dafür der **räumliche Anwendungsbereich**[6] der DSGVO, übrigens eine der wesentlichen Neuerungen gegenüber den bisherigen nationalen Datenschutzgesetzen. Alle Unternehmen, die innerhalb der Europäischen Union ihren Firmensitz oder eine Niederlassung haben fallen ebenso drunter, wie auch Unternehmen, die Daten von EU-Bürgern verarbeiten. Dabei ist es unerheblich, wenn diese ihren Sitz ausschließlich in einem Land außerhalb der EU haben (etwa in den USA). Kleiner Tipp: Europäische Unternehmen, die mit externen Datenverarbeitern (Dienstleistern) außerhalb Europas (USA, Indien usw.) zusammenarbeiten, müssen diese darauf drängen, dass sie sich ab Mai 2018 an die europäischen Regeln halten zu haben. Tun sie es nicht, trägt das Risiko der Auftraggeber, also das europäische Unternehmen.

Interessantes Detail am Rande: Auch die personenbezogenen Daten von Menschen, die sich zwar in der EU aufhalten aber nicht Staatsangehörige eines EU-Mitgliedstaates sind (so etwa auch Touristen) unterliegen dem DSGVO.

[4] https://dsgvo-gesetz.de/art-2-dsgvo
[5] https://dsgvo-gesetz.de/art-5-dsgvo
[6] https://dsgvo-gesetz.de/art-3-dsgvo

PERSONENBEZOGENE DATEN

Weil im Datenschutz immer wieder von **personenbezogenen Daten** die Rede ist: Dieser Begriff wird in der Datenschutz-Grundverordnung übrigens sehr weit gefasst und umfasst unter anderen Informationen wie Name, Adresse, Geburtsdatum, Telefonnummer, Bankdaten oder aber auch die IP-Adresse einer Person. Vorsicht: Es genügt hier bereits, wenn eine Informationen einer Person lediglich irgendwie zugeordnet und damit ein Personenbezug hergestellt werden **kann**.

Eine spezielle Untergruppe bilden zudem die sensiblen personenbezogenen Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit abzulesen sind. Auch genetische und biometrische Daten, die zur eindeutigen Identifizierung einer natürlichen Person beitragen, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung zählen dazu. Deren Verarbeitung unterliegt sehr strengen Maßstäben beziehungsweise ist generell untersagt – es sei denn, die Person willigt ein und die Datenverarbeitung fällt unter die in Artikel 9 Absatz 2 DSGVO definierten Ausnahmen (etwa für den Bereich Arbeitsmedizin). Keine Geltung hat die DSGVO übrigens für **anonyme Informationen**, das heißt für alle Informationen, die nicht einer natürlichen Person zugeordnet werden können. Auch die Daten Verstorbener unterliegen nicht mehr den Regelungen, allerdings können die Mitgliedstaaten eigene, konkretere Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.

03. PFLICHTEN FÜR UNTERNEHMEN

Nicht alles, was die DSGVO mit sich bringt, ist wirklich neu erfunden. Viele Verpflichtungen sind nämlich bereits vom Österreichischem Datenschutzgesetz (DSG 2000) her bekannt – wenngleich manches weniger rigoros bzw. unter anderem Namen ausgelegt wurde. Daraus lässt sich übrigens schlussfolgern, dass Unternehmen, die den Datenschutz schon bisher sehr ernst genommen haben, sich auch bei der Umstellung zur DSGVO erheblich leichter tun werden. Allerdings hält die Verordnung auch für diese datenschutztechnischen Vorzeigeunternehmen einige Stolperfallen bereit.

DATENSCHUTZ-FOLGEABSCHÄTZUNG

So etwa die **Pflicht zur Datenschutz-Folgenabschätzung**[7]. Eine solche ist immer dann durchzuführen, wenn ein hohes Risiko für die Rechte und Freiheiten der Personen durch die Verarbeitung der Daten besteht. Oder anders umschrieben: Wenn die Datenverarbeitung besonders sensibler Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen, einschließlich seiner Fähigkeiten, Leistungen oder seines Verhaltens zu bewerten. Für eine solche Folgenabschätzung müssen Unternehmen die geplanten Verarbeitungsvorgänge und Zwecke der Datenverarbeitung beschreiben sowie die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung und mögliche Risiken für die Rechte und Freiheiten betroffener Personen bewerten.

Und hier liegt leider auch der sprichwörtliche Hund begraben: Die DSGVO liefert nämlich nur die allgemeinen, eher schwammigen Vorgaben. Wie und nach welchen Kriterien die Folgen und Risiken für Betroffene abgeschätzt werden sollen und können bleibt weitgehend offen. Abgesehen davon, dass die (vermutlich notwendige) Konsultation der zuständigen Aufsichtsbehörde zu noch nicht abschätzbaren (negativen) Auswirkungen und zu vermehrter Bürokratie führen dürfte.

[7] https://dsgvo-gesetz.de/art-35-dsgvo
[8] https://dsgvo-gesetz.de/art-30-dsgvo

VERZEICHNIS VON VERARBEITUNGS-TÄTIGKEITEN

Erfreulicher ist da schon die Tatsache, dass es künftig keine Meldungen ans DVR (Datenverarbeitungsregister) mehr geben wird. Stattdessen werden Unternehmen ein internes **Verzeichnis von Verarbeitungstätigkeiten**[8] führen müssen. In diesem werden beispielsweise Namen und Kontaktdaten des Verantwortlichen, der Zweck der Datenverarbeitung, die Kategorien der betroffenen Personen und der personenbezogenen Daten, die Kategorien von Empfängern und eine Allgemeinbeschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen enthalten sein. Fehlt ein solches Verzeichnis, droht ein Bußgeld von bis zu 10 Mio. Euro bzw. bis zu zwei Prozent des Jahresumsatzes.

DATENSCHUTZBEAUFTRAGTER

Lange gestritten wurde darüber, ob nun jedes Unternehmen einen so genannten **Datenschutzbeauftragten**[9] bestellen muss. Seine Aufgabe ist es, auf die Einhaltung der datenschutzrechtlichen Vorgaben hinzuwirken sowie die gesetzmäßige Nutzung von EDV-Programmen im Unternehmen zu kontrollieren und zu überwachen[10]. Der Datenschutzbeauftragte ist in seiner Funktion zwar der Geschäftsleitung unterstellt, agiert aber weisungsfrei. Er ist zudem zur Verschwiegenheit verpflichtet und genießt einen zusätzlichen Kündigungsschutz[11].

Der österreichische Gesetzgeber hat sich in seiner nationalen Regelung übrigens dafür entschieden, bei der Bestellung eines Datenschutzbeauftragten nicht über die Mindestvorgaben der DSGVO hinaus zu gehen. Das heißt: Ein solcher muss nur in Betrieben verpflichtend bestellt werden, deren Kerntätigkeit in einer „umfangreichen regelmäßigen und systematischen Beobachtung von betroffenen Personen, umfangreichen Verarbeitung besonderer Kategorien von Daten („sensibler Daten“) oder von Daten über strafrechtliche Verurteilungen oder Straftaten besteht“. Selbstverständlich bleibt es jedem Unternehmen überlassen, auf freiwilliger Basis einen Datenschutzbeauftragten zu ernennen. Dieser genießt dann aber auch sämtliche Rechte und Pflichten.

MELDEPFLICHT BEI DATENSCHUTZ-VERLETZUNGEN

Tritt der schlimmste Fall der Fälle ein und es kommt zu Datenschutzverletzungen, etwa durch einen Hackerangriff, übel gesinnte (Ex-)Mitarbeiter oder den Verlust eines Datenträgers, dann sind Unternehmen laut DSGVO dazu verpflichtet, den Vorfall der Datenschutzbehörde und den betroffenen Personen zu melden. Der so genannten Pflicht zur „**Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde**“ ist binnen 72 Stunden nach Kenntnisnahme des Vorfalls nachzukommen[12]. Eine kleine Ausnahme gibt es jedoch, wenn die Datenschutzverletzung voraussichtlich kein Risiko für die persönlichen Rechte und Freiheiten der Betroffenen bedeutet – dann kann eine solche Meldung unterbleiben. Es bleibt aber noch abzuwarten, wie die Behörde die Formulierung „voraussichtlich kein Risiko“ definieren wird.

Gleichzeitig mit der Meldung muss das betroffene Unternehmen auch die Datenpanne einschließlich aller damit im Zusammenhang stehenden Fakten, deren Auswirkungen und die ergriffenen Maßnahmen dokumentieren. Fast schon unnötig zu erwähnen, dass bei einem Verstoß gegen die Meldepflicht ein Bußgeld von bis zu zehn Mio. Euro bzw. bis zu zwei Prozent des weltweit erzielten Jahresumsatzes verhängt werden kann.

Weitere Pflichten für Unternehmen ergeben sich zudem durch die erheblich erweiterten Rechte der Betroffenen, also jener Personen, um deren Daten es sich handelt. Um welche Rechte es hier konkret geht, lesen Sie im nächsten Kapitel.

[9] https://dsgvo-gesetz.de/art-37-dsgvo
[10] https://dsgvo-gesetz.de/art-39-dsgvo
[11] https://dsgvo-gesetz.de/art-38-dsgvo
[12] https://dsgvo-gesetz.de/art-33-dsgvo

04. INFORMATIONSPFLICHTEN & DIE RECHTE BETROFFENER

Modernisiert und kräftig erweitert werden durch die DSGVO die **Informationspflichten der Unternehmen** und die individuellen Rechte der Betroffenen, sprich jener identifizierten oder identifizierbaren natürlichen Person, um deren Daten es sich hierbei handelt. Alles in allem widmet man diesem Thema sogar das ganzes dritte Kapitel der Verordnung.

Konkret zu finden ist der umfangreiche Auskunftskatalog in den Artikeln 13 und 14 der DSGVO, wobei Artikel 13 regelt, welche Informationen Unternehmen liefern müssen, wenn man die Daten direkt von der betroffenen Person erhebt – beispielsweise im Zuge einer Newsletter-Anmeldung oder ähnlichen Vorgängen. In Artikel 14 werden dann jene Informationspflichten erläutert, wenn die Daten nicht bei der betroffenen Person erhoben werden. Eine genaue Übersicht über die zum Zeitpunkt der Datenerhebung zu liefernden Informationen erhalten Sie mit einem Klick auf den entsprechenden Artikel.

Sämtliche Informationen sind übrigens in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ zu übermitteln – oder mit anderen Wort: „Deppensicher“ zu gestalten. Lustigerweise ist – gemäß DSGVO – ausdrücklich auch eine Datenschutzerklärung in Piktogrammen (aber keine Smileys!) denkbar. Man darf allerdings gespannt sein, wie das dann wohl in der Praxis aussieht…

LEICHTERE AUSÜBUNG DER RECHTE

Eine Frage der praktischen Anwendung wird es auch sein, wie mit den **Rechten der Betroffenen**[13] umgegangen werden wird. Dem Willen des europäischen Gesetzgebers entsprechend, wurden in der DSGVO Modalitäten festgelegt, die einer betroffenen Person die Ausübung der Rechte erheblich erleichtern. Konkret handelt es sich dabei um das Recht auf Auskunft, Berichtigung, Einschränkung und Löschung von Daten – vieles davon ist allerdings auch dem jetzigen Datenschutzgesetz nicht fremd.

Die betroffene Person hat beispielsweise auch weiterhin das Recht, unverzüglich die **Berichtigung**[14] sie betreffender unrichtiger personenbezogener Daten zu verlangen. Gleiches gilt für die Vervollständigung unvollständiger personenbezogener Daten. Bereits bekannt müssten auch das **Recht auf Auskunft**[15] und das Widerspruchsrecht[16] gegen eine an sich rechtmäßige Datenverarbeitung sein.

Etwas komplizierter wird es dann schon beim **Recht auf Löschung der Daten**[17], wobei diese verlangt werden kann, wenn die Daten zu dem Zweck, zu dem sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr erforderlich sind, sie unrechtmäßig verarbeitet wurden oder die Einwilligung in eine weitere Speicherung widerrufen wurde. Das Problem ist jedoch, dass die DSGVO offenlässt, was man unter Löschung versteht: Reicht es, wenn man die Daten unkenntlich macht oder müssen sie vernichtet werden?

Noch viel weiter reicht das **Recht auf Vergessenwerden**, quasi eine exzessive Ausformung des Löschungsanspruches. Dieses Recht greift immer dann, wenn die verantwortliche Stelle die zu löschenden Daten öffentlich gemacht hat. Verlangt eine betroffene Person die Löschung aller Daten/Kopien und Links zu diesen Links zu diesen Daten, dann müssen ab sofort auch Dritte darüber in Kenntnis gesetzt werden. Das betrifft beispielsweise Dienstleister, an die man die Daten weitergeleitet hat, aber auch Suchmaschinen.

[13] https://dsgvo-gesetz.de/kapitel-3
[14] https://dsgvo-gesetz.de/art-16-dsgvo
[15] https://dsgvo-gesetz.de/art-15-dsgvo
[16] https://dsgvo-gesetz.de/art-21-dsgvo
[17] https://dsgvo-gesetz.de/art-17-dsgvo

Ein absolutes Novum der DSGVO ist das **Recht auf Datenübertragbarkeit**[18]. Dieses Recht gibt betroffenen Personen unter bestimmten Voraussetzungen einen Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten. Der Nutzer hat damit das Recht, Daten von einem Anbieter zu einem anderen „mitzunehmen". Schlagend wird das vor allem bei Energieversorgern, Banken oder Versicherungen, um den Wechsel zu einem anderen Anbieter zu erleichtern.

Sämtliche Maßnahmen und Anfragen müssen unverzüglich, längstens aber innerhalb eines Monats erledigt bzw. beantwortet werden. Unter Berücksichtigung der Komplexität bzw. einer sehr hohen Anzahl von Anfragen, kann diese Frist um weitere zwei Monate verlängert werden – der Antragssteller ist darüber gesondert zu unterrichten. Ebenso, wie er freilich auch über alle durchgeführten Maßnahmen zu informieren ist.

Sämtliche Informationen, Mitteilungen und Maßnahmen sind zudem unentgeltlich zur Verfügung zu stellen. Eine Ausnahme gibt's nur bei offenkundig unbegründeten oder exzessiven Anträgen (z.B., wenn Anfragen häufig wiederholt werden): Dann kann entweder ein angemessenes Entgelt verlangt werden oder das Unternehmen kann sich auch weigern, tätig zu werden. Doch Vorsicht: Ob die Anfrage des Betroffenen tatsächlich offenkundig unbegründet oder exzessiv war, hat der für die Verarbeitung Verantwortliche (also das Unternehmen) zu beweisen.

[18] https://dsgvo-gesetz.de/art-37-dsgvo

05. WICHTIGE BEGRIFFE

Im Sinne der DSGVO verwendeten Ausdrücke und deren Bedeutung (Überblick & Auszug[19]). Im Sinne der Übersichtlichkeit werden hier nur die geläufigsten Begriffe angeführt – eine vollständige Liste finden Sie hinter dem in der Fußnote angeführten Link:

1. PERSONENBEZOGENE DATEN

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

2. VERARBEITUNG

Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

3. EINSCHRÄNKUNG DER VERARBEITUNG

die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

4. PROFILING

Jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

5. PSEUDONYMISIERUNG

Die Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

[19] https://dsgvo-gesetz.de/art-4-dsgvo/

6. DATEISYSTEM

Jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

7. VERANTWORTLICHER

Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel dieser Verarbeitung durch das EU-Recht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

8. AUFTRAGSVERARBEITER

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

9. EMPFÄNGER

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem EU-Recht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger. Die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

10. DRITTER

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

11. EINWILLIGUNG

Jede freiwillig, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

12. VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN

Eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

[20] https://dsgvo-gesetz.de/art-27-dsgvo

13. GESUNDHEITSDATEN

Personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

14. VERTRETER

Eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27[20] DSGVO bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt.

15. UNTERNEHMEN

Eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

16. AUFSICHTSBEHÖRDE

Eine von einem Mitgliedstaat gemäß Artikel 51[21] DSGVO eingerichtete unabhängige staatliche Stelle. In Österreich ist das die Datenschutzbehörde (https://www.dsb.gv.at/).

17. MASSGEBLICHER UND BEGRÜNDETER EINSPRUCH

Ein Einspruch im Hinblick darauf, ob ein Verstoß gegen die Verordnung vorliegt oder nicht oder ob die beabsichtigte Maßnahme gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen.

[20] https://dsgvo-gesetz.de/art-27-dsgvo

[21] https://dsgvo-gesetz.de/art-51-dsgvo

06. SCHLAGWÖRTER / INDEX

A
Anonyme Informationen 5

Auftragsverarbeiter 10

D
Dateisystem 10

Datenschutzbeauftragter 6

Datenschutzbehörde 6
Aufsichtsbehörde 11

Datenschutz-Folgenabschätzung 5

Datenverarbeiter 4
Dienstleister 4

Dritter 14

E
Einwilligung 10

Empfänger 10

G
Gesundheitsdaten 11

I
Informationspflichten der Unternehmen 7

M
Maßgeblicher und begründeter Einspruch 11

Meldung von Verletzungen
des Schutzes personenbezogener Daten 6

P
Personenbezogene Daten 4

Profiling 9

Pseudonymisierung 13

R
Räumlicher Anwendungsbereich 4

Recht auf Auskunft 7

Rechte der Betroffenen 7
Berichtigung 7
Datenübertragbarkeit 8
Löschung der Daten 7
Vergessenwerden 7
Widerspruchsrecht 7

S
Sachlicher Anwendungsbereich 4

U
Unternehmen 11

V
Verantwortlicher 10

Verarbeitung 9
Datenverarbeitung 5
Einschränkung der Verarbeitung 9

Verletzung des Schutzes
personenbezogener Daten 10

Vertreter 11

Verzeichnis von Verarbeitungstätigkeiten 6
DVR-Register 6

KONTAKT

DAMIAN IZDEBSKI
Founder & CEO

+43 664 800 80 800
+43 1 34 34 333 800
di@techbold.at

GERALD REITMAYR
Chief Operating Officer

+43 664 800 80 900
+43 1 34 34 333 900
gr@techbold.at

SEBASTIAN HINTERSEER
Head of Sales

+43 664 800 80 502
+43 1 34 34 333 502
sh@techbold.at

TECHBOLD TECHNOLOGY GROUP AG
DRESDNER STRASSE 89, 1200 WIEN
+43 1 34 34 333 | office@techbold.at